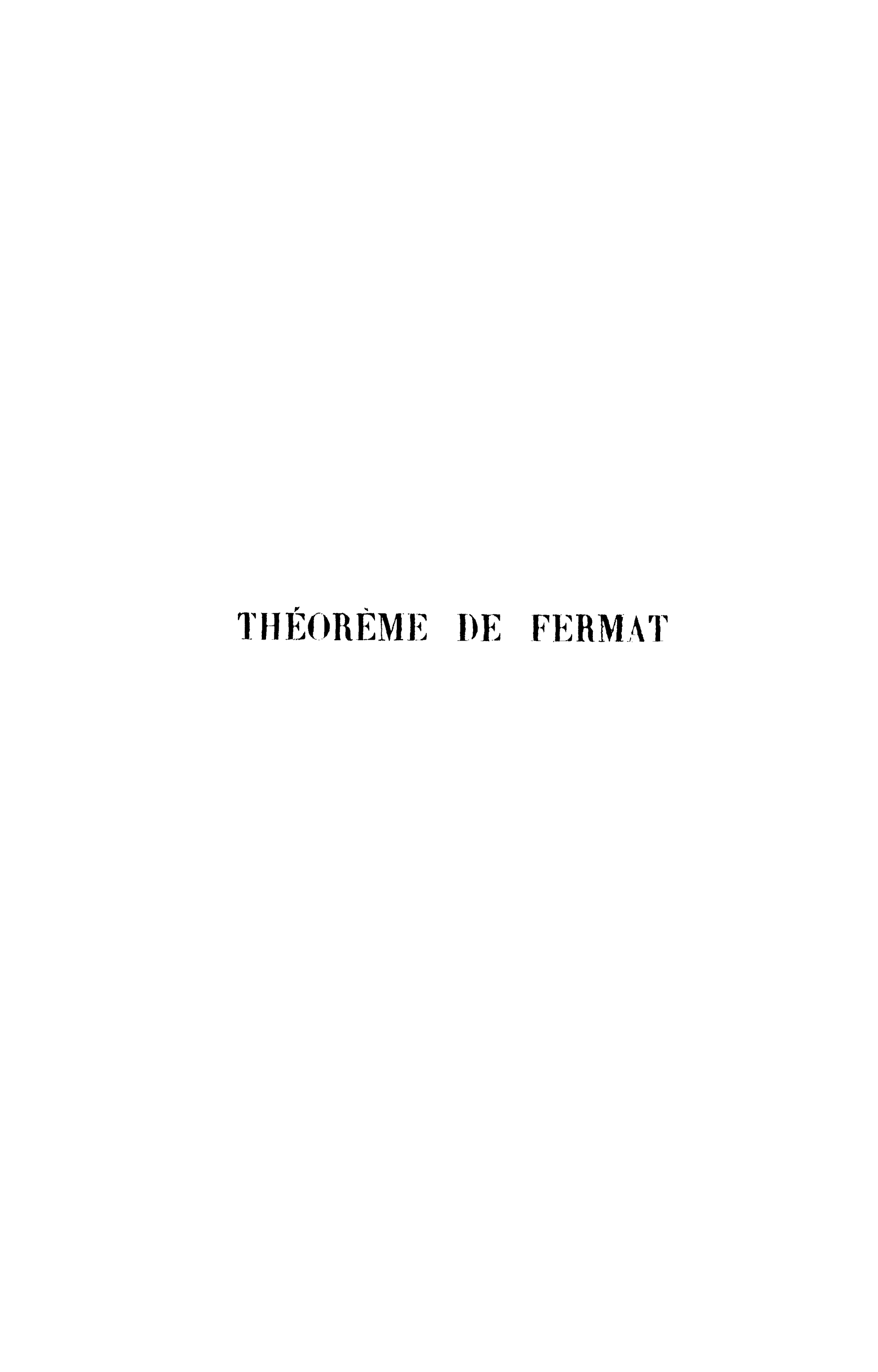


THÉORÈME DE FERMAT

DU MÊME AUTEUR

A LA MÊME LIBRAIRIE

Cours de Mathématiques spéciales sous forme de problèmes (*algèbre et analyse, trigonométrie, géométrie analytique, mécanique, géométrie descriptive*), à l'usage des élèves de Mathématiques spéciales. — 2ᵉ édit. Vol. 25/16ᶜᵐ avec fig. . . . . **32** fr. »

Marcel Noguès raconté par ses parents. — Vol. 20/13ᶜᵐ. . **8** fr. »

R. NOGUÈS

Ancien élève de l'École Normale supérieure,
Professeur honoraire de Mathématiques spéciales
au lycée Janson-de-Sailly.

THÉORÈME DE FERMAT

SON HISTOIRE

PARIS
LIBRAIRIE VUIBERT
Boulevard Saint-Germain, 63

1932



A LA MÉMOIRE DE MON FILS MARCEL

INTRODUCTION

Fermat a donné un énoncé manuscrit de son théorème sur la marge d'un exemplaire des Œuvres de Diophante éditées par Bachet: *Cubum in duos cubos aut quadrato-quadratum in duos quadrato-quadratos et generaliter nullam in infinitum, ultra quadratum, potestatem in duas ejusdem nominis fas est dividere.*

Cujus rei demonstrationem mirabilem sane detexi; hanc marginis exiguitas non caperet.

C'est dire :

L'équation $x^n + y^n = z^n$, *où* n *est un entier quelconque, plus grand que* 2, *n'a pas de solutions entières en* x, y, z, *autres que celles où une inconnue a la valeur zéro.*

Pour $n = 2$, les solutions, en nombre infini, sont données par la formule

$$(a^2 - b^2)^2 + (2ab)^2 = (a^2 + b^2)^2,$$

où a, b sont deux entiers quelconques. Si a, b sont premiers entre eux, l'un pair, l'autre impair, $a^2 - b^2$, ab, $a^2 + b^2$ seront premiers entre eux, deux à deux.

Fermat n'a pas laissé sa démonstration pour $n = 4$; il en a probablement communiqué le principe à Frénicle de Bussy, dont la démonstration, la première imprimée du théorème de Fermat, est de 1676 (*Traité des triangles rectangles en nombres*).

Le théorème de Fermat, démontré pour $n = 4$, l'est, par cela même, quand n est une puissance de 2. En effet, ces

puissances, à partir de 8, sont des multiples de 4, et l'on a $x^{4m}+y^{4m}=z^{4m}$, c'est-à-dire $(x^m)^4+(y^m)^4=(z^m)^4$.

Il suffit donc d'essayer la démonstration pour les exposants premiers, puisque tout entier est multiple d'un nombre premier. Il est évident, d'ailleurs, que x, y, z peuvent être supposés premiers entre eux deux à deux et qu'un seul est pair.

Jusqu'à ce jour, le théorème n'a été démontré que pour des exposants particuliers ; ainsi, dans la première centaine, il l'a été pour tous les nombres premiers, 59 et 67 exceptés.

Tant qu'il ne l'aura pas été dans toute sa généralité, ne convient-il pas, afin de susciter de nouvelles recherches, de rappeler dans leur ordre chronologique celles qui ont été déjà faites et de montrer où en est la question ?

Tel est l'objet de cette publication.

Le livre comprend une partie historique et une partie mathématique. Dans la première, les méthodes employées, les résultats obtenus, les noms des auteurs, l'indication de leurs œuvres sont présentés au lecteur. Dans la seconde, les démonstrations, exposées et résumées, lui permettront, sa curiosité ayant été éveillée, de connaître tout ce qui a été fait et d'en apprécier la valeur.

On l'a dit : « Le théorème de Fermat est un défi jeté à l'intelligence humaine. » Qui le relèvera ?

En attendant, l'intérêt particulier du théorème de Fermat est qu'il a donné naissance à la théorie des Nombres algébriques.

THÉORÈME DE FERMAT

PREMIÈRE PARTIE

CHAPITRE I

PRÉLIMINAIRES

§ I. — Œuvres de Fermat.

Pierre Fermat naquit, en août 1601, à Beaumont-en-Lomagne, village situé entre Toulouse et Lectoure, dans le Tarn-et-Garonne.

Il mourut, en janvier 1665, à Castres où l'avaient appelé ses fonctions.

Fermat termina ses études à Toulouse.

« Tandis que sa carrière de conseiller à la Cour de Toulouse s'écoulait obscurément, il s'acquit, par la communication en manuscrits de traités composés en latin et par sa correspondance en français avec quelques savants, ayant trait exclusivement aux questions mathématiques, le renom d'un géomètre hors de pair.

« En dehors de ses aptitudes mathématiques, Fermat possédait une très grande érudition.

« Son caractère se montre, d'après sa correspondance, affable, peu susceptible, sans orgueil, mais avec cette petite pointe de vanité que Descartes, son contraire à tous égards, qui mêlait l'aigreur à la polémique, caractérisait en disant : « Monsieur de Fermat est Gascon ; moi, je ne le suis pas. »

« Ce n'était pas par la voie de l'imprimerie que son nom s'était répandu dans le monde savant. Lui-même n'avait fait imprimer qu'une dissertation géométrique, tout en gardant l'anonyme. Cet opuscule parut en 1660.

« Il a laissé presque tous ses théorèmes sans démonstrations. C'était l'esprit du temps de se proposer, les uns aux autres, des problèmes. On cachait le plus souvent sa méthode afin de se réserver des triomphes nouveaux, tant pour soi que pour sa nation; car il y avait surtout rivalité entre les géomètres français et les géomètres anglais. De là, il est arrivé que la plupart des démonstrations de Fermat ont été perdues. »

(LEGENDRE, Préface de la première édition de sa *Théorie des Nombres*, 1823, et insérée dans la troisième.)

Son *Introduction aux Lieux plans*, à l'instar d'Apollonius, est un traité concis de Géométrie analytique, comprenant la théorie de la droite et des courbes du second degré. A la même époque, 1636, fut publiée pour la première fois, à Leyde, la Géométrie de Descartes.

On lui doit un *Traité du contact des Sphères*, une courte notice sur les Porismes (EUCLIDE). Malheureusement, Fermat se bornait à communiquer ses découvertes à ses amis.

Les deux *Mémoires sur la théorie des Maximis et sur les Tangentes et les Quadratures* établissent ses droits à l'invention du calcul différentiel et du calcul intégral. D'Alembert, Lagrange, Laplace, Fourier font remonter à ces deux mémoires l'origine du calcul infinitésimal (LAGRANGE, *Calcul des Variations*, 8ᵉ leçon).

Plus de cinq ans après la publication de ces mémoires, le dernier discuté par Descartes, Leibnitz fit paraître dans les « Actes de Leipzig » son Mémoire sur le calcul différentiel, sous le même titre, *Methodus pro maximis*. « On peut dire que Leibnitz lui-même n'eût point contredit à ce jugement; car on lit dans une de ses lettres à Wallis ce passage, où respire la sérénité qui convenait à son grand esprit, à sa noble intelligence : *Quod calculum differentialem attinet; fateor*

multa et esse communia cum iis quœ et tibi et Fermatio aliisque, imo jam ipsi Archimedi, erant explicata, etc. » (CHASLES, Séance d'ouverture à la Faculté des Sciences de Paris, 22 décembre 1846.)

« C'est dans la Science des Nombres que Fermat se fraya une voie nouvelle. Diophante, d'Alexandrie, avait inauguré cette Science ; son ouvrage était écrit en grec. Sur treize livres, six ont seuls été conservés ; ils ne furent connus en Europe qu'au commencement du XVe siècle. En 1575, l'Allemand Holzmann en publia une traduction latine. Bachet de Méziriac, à qui l'on doit la résolution en nombres entiers de l'équation indéterminée du premier degré, perfectionna cette traduction et la fit suivre d'un *Commentaire* prolixe, mais lumineux, en 1626. C'est sur un exemplaire de ce Commentaire que Fermat inséra ses *Observations* marginales, écrites en latin. » (BRASSINNE, *Précis.*)

Fermat s'est aussi occupé, à l'exemple de Frénicle, son contemporain, des *Carrés magiques.* Il cite plusieurs exemples de carrés magiques, mais il ne démontre rien. « J'ai découvert, écrit-il à Mersenne, la question du carré 22 ; en sorte qu'en enlevant trois enceintes, il reste magique ; et, du restant, encore deux, et qu'il demeure magique ; et puis, une seule, du reste, à la même condition. Je me contenterai pour ce coup de vous envoyer le carré qui reste après les trois premières et les deux secondes enceintes ôtées. Parce que le temps me manque, je diffère à vous envoyer les cinq enceintes qui manquent, jusqu'au départ du prochain courrier. »

Fermat n'avait fait qu'effleurer la Mécanique et la Physique. Il s'occupait d'un grand ouvrage qui devait, disait-il, contenir beaucoup de belles propriétés des nombres.

Son fils, SAMUEL FERMAT, a publié à Toulouse, en 1679, sous le titre *Opera varia*, les Mémoires de son père.

En 1861, cet ouvrage a été réimprimé à Berlin.

En 1670, Samuel Fermat fit paraître une édition, in-folio, de Diophante, sous le titre : *Diophanti Alexandrini Arithmeticorum Libri sex et de numeris multangulis Liber unus Commentariis C. G. Bacheti et Observationibus D. P. de Fermat, Senatoris Tolosani.*

« L'intérêt de l'édition de Samuel Fermat provient essentiellement des annotations que Fermat avait inscrites sur les marges d'un exemplaire, aujourd'hui perdu, sur le Diophante de Bachet, annotations que son fils a reproduites à leur place.

Fermat, qui n'avait point de cahier de notes et ne conservait pas de manuscrits, inscrivait des remarques sur les marges des livres qui lui appartenaient, quelle que fût la nature de ces livres. » (Tannery, Henry.)

Samuel a inséré dans son livre *Diophante* un traité, rédigé par Billy, sous le titre *Inventum novum,* où sont recueillies et développées lesdites *Observations* de son père.

Montucla, dans son Histoire des Mathématiques, indique succinctement les principales questions traitées par Fermat.

Dans un ouvrage, couronné par l'Académie de Toulouse, *Influence de Fermat sur son siècle* (1784), Genty a apprécié le cachet particulier de son génie.

En 1843, le Ministre Salvandy présenta aux Chambres un projet de loi pour la réimpression, aux frais de l'État, des Œuvres complètes de Fermat. Le crédit demandé de 15 000 francs fut voté. Mais les difficultés provenant de la traduction des textes latins de forme abandonnée et de notations incommodes empêchèrent l'effet de ce vote.

E. Brassinne, professeur à l'école d'artillerie de Toulouse, a publié à Toulouse, en 1853, un *Précis des Œuvres mathématiques de Fermat et de l'Arithmétique de Diophante.*

Paul Tannery et Charles Henry ont publié, sous les auspices du Ministère de l'Instruction publique, en 1891, les *Œuvres de Fermat.* Cette publication comprend quatre volumes in-4° : le premier renferme les œuvres mathéma-

tiques diverses, en latin, et les observations sur Diophante; le deuxième et le troisième renferment la correspondance de Fermat, en français; le quatrième, un supplément à la correspondance et des documents inédits avec notes sur les nouveaux manuscrits par C. de Waard.

§ II. — Méthode de la descente infinie.

A la fin du VI[e] Livre de *Diophante,* Bachet a placé une série de problèmes. Fermat ajoute au 20[e] problème une *Observation* : « L'aire d'un triangle rectangle, exprimée en nombres entiers, ne peut être égale à un carré. — Nous placerons ici la démonstration, de notre invention, de ce théorème, que nous avons découverte après une laborieuse et pénible méditation. Ce genre de démonstration produira de merveilleux progrès dans les questions arithmétiques. »

Dans une lettre de Fermat à Carcavi (1659), qui la communiqua à Huygens (Tannery, t. II, page 43), on lit : « Et, pour ce que les méthodes qui sont dans les livres étaient insuffisantes à démontrer des propositions si difficiles, je trouvai enfin une route tout à fait singulière pour y parvenir. J'appelai cette manière de démontrer *la descente infinie,* et je m'en servis au commencement pour démontrer les propositions négatives, comme, par exemple, qu'il n'y a aucun nombre moindre de l'unité, qu'un multiple de trois, qui soit composé d'un carré et du triple d'un autre carré; qu'il n'y a aucun triangle rectangle, exprimé en nombres entiers, dont l'aire est un carré.

« La preuve se fait par απαγωγην είς αδυνατον, (réduction à l'absurde), en cette manière : s'il y avait un triangle en nombres entiers qui ait une aire égale à un carré, il y aurait un autre triangle, moindre que celui-là, qui aurait la même propriété. S'il y en avait un second, moindre que le premier, qui eût cette même propriété, il y en aurait, par un pareil raisonnement, un troisième, moindre que le second, qui aurait la même propriété et enfin un quatrième, un cinquième, et à l'infini en descendant. Or, est-il qu'étant donné un

nombre entier il n'y en a point infinis entiers en descendant moindres que celui-là. D'où on conclut qu'il est donc impossible qu'il y ait aucun triangle rectangle dont l'aire soit carrée.

« Je n'ajoute pas la raison d'où j'infère que, s'il y avait un triangle rectangle de cette nature, il y en aurait un autre de même nature moindre que le premier, parce que le discours en serait trop long et que c'est là tout le mystère de ma méthode. Je serai bien aise que les Pascal et les Roberval et tant d'autres savants la cherchent sur mes indications.

« Je fus longtemps sans pouvoir appliquer ma méthode aux propositions affirmatives parce que le tour et le biais pour y parvenir est de beaucoup plus malaisé. De sorte que lorsqu'il me fallut prouver que tout nombre premier qui surpasse de l'unité un multiple de 4 est composé de deux quarrés, je me trouvai en belle peine. Mais de nouveaux principes me permirent de réussir. Mon raisonnement sur les questions affirmatives est tel : si un pareil nombre, pris à discrétion, n'est point composé de deux quarrés, il y aura un nombre de même nature moindre que le donné et ensuite un troisième encore moindre, etc., en descendant à l'infini jusqu'à ce que vous arriviez à 5, qui est le moindre, lequel il s'en suivrait n'être pas composé de deux quarrés, ce qu'il est pourtant, d'où on doit inférer, par la déduction à l'impossible, que tous ceux de même nature sont, par conséquent, composés de deux quarrés.

« J'ai ensuite considéré certaines questions qui, bien que négatives, ne restent pas de recevoir une grande difficulté, la méthode pour y pratiquer la descente étant tout à fait différente des précédentes, comme il sera aisé d'éprouver. Telles sont les suivantes : Il n'y a aucun cube divisé en deux cubes.

« Il n'y a qu'un seul quarré (25) en entiers, qui, augmenté du binaire, fasse un cube.

« Il n'y a que deux quarrés (4 et 12), lesquels, augmentés de 4, fassent un cube. »

Lagrange s'est servi de la descente, non pour prouver l'im-

possibilité de certaines questions, mais pour trouver les solutions les plus simples d'équations possibles.

Lejeune-Dirichlet (*Journal für die reine und angewandte Mathematik*, *Journal de Crelle*, 1828), dans un mémoire lu devant l'Académie des Sciences de Paris et approuvé par les commissaires Lacroix, Legendre, écrit : « Pour résoudre ces équations indéterminées, on est naturellement conduit à une ou à plusieurs formules quadratiques qu'il s'agit d'égaler à des puissances parfaites. On satisfait ensuite de la manière la plus générale à cette condition en exprimant les indéterminées par d'autres indéterminées, dont les premières deviennent des fonctions entières, et il se trouve, au moins dans tous les cas où la méthode dont il s'agit réussit, que les nouvelles indéterminées, ou d'autres quantités qui en dépendent d'une manière très simple, satisfont à une équation semblable à l'équation proposée.

« Comme les nouvelles indéterminées sont en même temps plus petites que les indéterminées primitives, l'impossibilité de l'équation proposée se trouve établie ; car il est évident que, si elle était possible, on aurait le moyen d'établir une suite décroissante et indéfinie de nombres entiers, ce qui implique contradiction.

« C'est de cette manière que Fermat, Euler ont prouvé l'impossibilité de plusieurs équations du troisième et du quatrième degré. »

Mirimanoff (*Journal de Crelle*, t. CXXVIII, p. 45, 1905) écrit, au sujet de l'équation $x^n + y^n + z^n = 0$: « Deux cas : x, y, z non divisibles par n, ou x divisible par n. Dans le premier cas, l'impossibilité, au moins pour les nombres n considérés jusqu'à présent, a pu être établie par des méthodes directes, tandis que le second semble exiger l'emploi d'un procédé particulier, dont s'est déjà servi Fermat et qui est désigné sous le nom de Descente. »

En 1922, Mordell (*On the rational solutions of the indeter-*

minate equations of the third and fourth degrees, Proc. of the Cambridge Philos. soc., t. XXI, p. 179), et André Weil (*l'Arithmétique sur les Courbes algébriques,* Thèse, Paris, 1928) ont appliqué la Descente infinie.

§ III. — Le théorème de Fermat est-il exact?

Depuis Fermat jusqu'à Euler, les géomètres, livrés entièrement à l'application des nouveaux calculs, ne s'occupèrent point de la théorie des nombres. Euler, le premier, s'attacha à cette partie ; mais le théorème de Fermat n'a pas encore été démontré, aussi sa vérité a pu être contestée.

Dans le numéro du 10 mars 1807 du Journal des Savants de Gœttingue, Gauss écrit : « L'arithmétique supérieure a ceci de particulier que ses plus beaux théorèmes se trouvent aisément par induction, tandis qu'on n'en trouve la démonstration qu'avec beaucoup de peine. Ainsi, l'un des plus grands mérites d'Euler est d'avoir démontré plusieurs des théorèmes de Fermat, que celui-ci avait obtenus, ce semble, par induction. »

Et le 12 mai 1808, Gauss insiste (*Œuvres*, t. II, p. 159, 2e édition) : « Les plus belles propriétés des nombres, et, en particulier, la loi de Réciprocité des résidus quadratiques, sont faciles à trouver par induction, mais très difficiles à démontrer. Fermat affirme avoir la démonstration de ses théorèmes ; aussi nous ne pouvons pas savoir s'il ne s'est pas trompé. »

Réfutation de Mansion, professeur à l'Université de Gand (*Nouvelle Correspondance mathématique,* t. V, p. 88, 1879) :

« Fermat est arrivé par induction, sans doute, mais par une induction basée sur une démonstration partielle, à sa proposition : $2^{2^n}+1$ est premier. Il a pensé qu'elle était vraie ; il l'a écrit à ses amis, mais il n'a jamais dit qu'il en avait une démonstration. Il s'exprime ainsi dans la lettre du 18 octobre 1640 à M. X. X. : « Comme je ne suis pas capable

de m'attribuer plus que je ne sais, je dis avec la même franchise ce que je ne sais pas ; que je n'ai pu encore démontrer l'exclusion de tous les diviseurs en cette belle proposition que je vous ai envoyée et que vous m'avez confirmée touchant les nombres 3, 5, 17, 257, 65537, etc. ; car, bien que je réduise l'exclusion à la plupart des nombres et que j'aie même des raisons probables pour le reste, je n'ai pu encore démontrer nécessairement la vérité de cette proposition. »

« Quatorze ans plus tard, dans une lettre à Pascal, 29 août 1654, il revient sur la même question : « Songez cependant, si vous le trouvez à propos, à cette proposition : les puissances carrées de 2, augmentées de l'unité, sont toujours des nombres premiers, $2^2+1=5$, $2^{2^2}+1=17$, $2^{2^3}+1=257$, $2^{2^4}+1=65537$, sont premiers, et ainsi à l'infini. C'est une proposition de laquelle je vous réponds. La démonstration en est très malaisée, et je vous avoue que je n'ai pu encore la trouver pleinement ; je ne vous la proposerais pas pour la chercher si j'en étais venu à bout. »

« Ainsi, Fermat affirme à plusieurs reprises et à bien des années d'intervalle qu'il n'a pu démontrer cette proposition. De quel droit, dès lors, peut-on dire que parfois il s'est fait illusion sur la valeur de ses preuves ? Les lettres de Fermat prouvent précisément le contraire de l'assertion de Gauss, quand il s'agit de $2^{2^n}+1$.

« Si Fermat était allé jusqu'à $2^{2^5}+1$, à savoir 4294067297, il aurait pu constater que ce nombre est divisible par 641. Euler a prouvé que $2^{2^6}+1$, à savoir 18446744073709551617 est divisible par 274 177, et Ed. Lucas que $2^{4096}+1$ est divisible par 114 629.

« D'ailleurs, quoi que dise Gauss, ce n'est pas un mince mérite de trouver, même par induction, des théorèmes généraux d'arithmétique supérieure, comme la loi de Réciprocité ou comme la célèbre proposition de Fermat. L'histoire de la loi de Réciprocité le prouve bien. Euler la publia dans toute sa généralité en 1784, et, cependant, Legendre et Gauss, qui avaient en mains ce dernier travail d'Euler, le méconnurent,

à tel point que chacun d'eux la retrouva par induction, le premier en 1785, le second en 1796, sans se douter de la découverte antérieure d'Euler.

« Mais, dira-t-on, Fermat parle de ses démonstrations comme si elles étaient relativement courtes ; or, celles que les géomètres les plus illustres ont données de ses théorèmes sont toujours assez étendues et quelques-unes supposent une longue chaîne de propositions préliminaires. Cela prouve simplement que l'on n'a pas retrouvé sa méthode. Celles qui la remplacent sont plus compliquées, peut-être parce qu'elles sont fécondes. On peut d'ailleurs arriver à un même but par plusieurs chemins, les uns courts, les autres plus longs. Ainsi, la première démonstration de la loi de Réciprocité, trouvée en 1796 par Gauss, après une année d'efforts, occupe une grande partie de la quatrième section des *Disquisitiones* et suppose connues une bonne partie des sections précédentes. La démonstration de Zeller, publiée en 1852, n'occupe que deux pages. Avec quelques modifications de détail, on peut la rendre accessible à quiconque connaît les premiers éléments de la théorie des nombres, elle aurait pu être trouvée par Fermat, il y a deux siècles, tout comme elle l'a été par Zeller, il y a quelques années. » (Démonstration de Zeller dans la *Nouvelle Correspondance Mathématique*, t. II, dans *Messenger*, t. V.)

Déjà, Libri en 1849 (*Monographies diverses*, n° 8) avait précédé Mansion et s'exprimait ainsi :

« Des mathématiciens, qui avaient fait de vains efforts pour démontrer le théorème prouvé par Fermat, ont voulu jeter quelque doute sur la réalité des démonstrations qu'il déclarait possibles, et ils ont supposé que ce grand géomètre était parvenu à certains résultats plutôt par induction et un peu au hasard que par une analyse rigoureuse de la question. Certes, si Fermat n'avait laissé que des théorèmes sans démonstrations, le doute serait, à la rigueur, possible ; mais, quand il s'agit d'un homme aussi éminent, qui a fait d'autres découvertes dont il a donné des démonstrations qu'il n'a pas

publiées et que nous connaissons parce que tous ses manuscrits n'ont pas été perdus, d'un homme auquel Pascal écrivait : « Je vous tiens pour le plus grand géomètre de toute l'Europe », il faut admettre que, ces vérités, il les avait démontrées rigoureusement par des méthodes qui lui étaient propres et que nous ignorons.

« Deux causes principales nous ont privés de ces démonstrations : l'aversion que Fermat manifeste constamment contre toute publicité qui porterait son nom, et les obstacles que son fils, qui n'était pas mathématicien, rencontra lorsqu'il voulut rassembler les manuscrits dispersés de son père et lorsqu'il chercha un savant capable de diriger l'édition. « J'ay si peu de commodité, écrivait-il à Mersenne, d'écrire mes démonstrations que je me contente d'avoir découvert la vérité et de savoir le moyen de la prouver lorsque j'auray le loisir de le faire. »

« Ses amis étaient Pascal, Descartes, Roberval, Frénicle, Wallis, Torricelli, Huygens, Mersenne, etc. Il ne gardait même pas copie des démonstrations qu'il leur adressait.

« Si le *Diophante* que possédait Fermat avait été non rogné, peut-être aurait-il pu, à cet endroit, comme il l'avait fait ailleurs, esquisser rapidement une démonstration. »

Autre protestation de Smith, professeur à l'Université d'Oxford (*Collected mathematical Papers*, t. I, p. 131, 1894) :

« Quand nous considérons l'état de l'Analyse à cette époque, il est surprenant qu'il ait réussi à créer des méthodes que les mathématiciens venus après n'ont pu découvrir ; néanmoins, ce n'est pas une raison pour le soupçonner d'être capable de mensonge ou d'avoir pris une apparence pour une preuve réelle. Ces soupçons sont réfutés non seulement par la réputation d'honneur et de franchise dont il jouissait parmi ses contemporains et par le témoignage de rare clarté d'esprit que fournissent ses écrits connus, mais encore par les faits de la cause elle-même.

« Gauss s'exprime désobligeamment sur Fermat. »

Dans son *Observation* à propos de l'aire du triangle rectangle, Fermat dit encore : « L'exiguité de la marge nous empêche d'insérer la démonstration complète et plus amplement expliquée. » Legendre l'ayant complétée, la sincérité de Fermat reçoit ici confirmation.

Elle est aussi confirmée par la déclaration d'Edouard Lucas au sujet du carré magique de 22 : « Fermat n'a pas fait connaître les cinq enceintes enlevées, et elles ont été reconstituées. Nous donnons la restauration complète de ce carré ; elle a été faite d'une manière fort remarquable par M. V. Cacoz, commandant d'artillerie en retraite ; mais, nous espérons donner le nombre de solutions du problème, d'après les indications de Fermat. — Dans une autre lettre à Mersenne, Fermat avoue que ses méthodes pour les carrés magiques, comme pour d'autres sujets, conduisent à de grands calculs.

« Quoi qu'il en soit, la théorie complète des carrés magiques paraissait une énigme lorsque nous avons eu le bonheur de mettre la main sur des manuscrits originaux de Fermat. Ces manuscrits se composent de quatorze cahiers et de feuillets détachés. La présente rédaction a pour but de montrer la marche suivie par Fermat, d'après l'étude des dessins et des carrés du manuscrit. » (*Récréations mathématiques,* t. IV, p. 89, 1894.)

Dans l'introduction de sa *Théorie des nombres* (1891), E. Lucas remarque que le théorème de Fermat avait été énoncé pour $n = 3$, avant Fermat, par les algébristes marocains ; il cite les principaux mathématiciens ayant cherché à résoudre « ce problème qui semble jeté comme un perpétuel défi à l'intelligence humaine » et, parmi eux, « Gauss lui-même, bien qu'il n'y fasse aucune allusion dans ses *Disquisitiones* ; nous en donnerons une preuve irréfutable : c'est la VIIe section, dans laquelle il transforme de tant de manières le quotient de la division de $x^p - y^p$ par $x - y$. »

Dans la préface, Lucas appelle Fermat notre *divus arithméticus,* et cite, au sujet de l'Arithmétique de Diophante, ce

jugement de Gauss : « La science est bien plus redevable aux Modernes, parmi lesquels peu d'hommes, à la vérité, mais tous dignes d'une gloire immortelle, Fermat, Euler, Lagrange, Legendre (et un petit nombre d'autres) ont ouvert l'entrée de cette science divine et ont découvert la mine inépuisable de richesses qu'elle renferme. » (Préface des *Disquisitiones*, d'après la traduction de Poullet-Delisle, Paris, 1807.)

Aux manuscrits trouvés par Edouard Lucas il faut en ajouter d'autres. En effet, on lit dans les Comptes rendus de l'Académie des Sciences du 16 septembre 1839 cette communication : M. Libri annonce à l'Académie qu'il vient de retrouver les manuscrits de Fermat dont les Géomètres regrettaient depuis si longtemps la perte. Ces manuscrits font partie d'une collection assez volumineuse dont M. Libri vient de faire l'acquisition grâce à l'obligeante intervention de Monsieur le capitaine Didéon, professeur à l'école d'application de Metz. La collection entière semble avoir été formée par Arbogast ; elle contient un nombre considérable de pièces inédites des plus illustres géomètres, parmi lesquels on peut citer Descartes, Roberval, Jean Bernoulli, L'Hospital, Moivre, Euler, d'Alembert, etc. Ils se composent : 1° de quelques cahiers de géomètres, qui paraissent autographiés ; 2° d'une copie de lettres de Fermat à Roberval, à Mersenne, etc. Il n'y a pas la démonstration de l'équation $x^n + y^n = z^n$, et tout prouve qu'elle n'existait pas dans les manuscrits de Mersenne, d'où ces copies ont été tirées.

M. Eugène Cahen semblerait, au contraire, se rallier à l'opinion de Gauss (*Théorie des nombres*, t. II, p. 590, 1924). « Mais il est plus que probable que cette démonstration n'était pas valable, puisque lui-même n'a pas jugé à propos de la faire connaître et qu'aucune démonstration n'a pu être retrouvée malgré les efforts des plus grands mathématiciens et les progrès considérables de la théorie des nombres depuis le temps de Fermat. »

« D'après ce que nous savons du caractère de Fermat, il est certain qu'il eut l'impression d'être en possession d'une démonstration méritant d'être signalée. Il n'en reste pas moins vrai qu'il est possible qu'il se soit mépris sur la valeur de cette démonstration ; car les plus grands mathématiciens ont commis des erreurs de ce genre. » (L. J. MORDELL, 1929)(1).

Dans le tome XXXVI des *Atti dell' Academia Pontificia*, on lit, sous la rubrique *opere venute in dono :* A. Marre, Appréciation nouvelle et singulière du caractère du Grand Fermat par C. Henry. Simple note de M. MARRE. Paris, 1883, in-8°.

(1) A défaut de démonstration on ne peut pas espérer tomber sur une solution particulière. En effet, écrivant $y^n \pm x^n = z^n$, on peut supposer z pair. Or, $y^n \pm x^n$ est le produit de deux facteurs, dont un seul, $y \pm x$, est pair, et, par conséquent, divisible par 2^n. Donc, pour $n = 59$, 67, par exemple, y, au moins, aurait plus de 18 et 20 chiffres.

CHAPITRE II

DE FERMAT A LEGENDRE

§ I. $x^4 + y^4 = z^4$, par FERMAT.

La première démonstration particulière du théorème est de Fermat lui-même pour $n = 4$.

Dans une de ses notes sur Diophante (édition citée de *Diophante*, p. 339) où il prouve que l'aire d'un triangle rectangle en nombres entiers ne saurait être égale à un carré, Fermat démontre par cela même l'impossibilité des équations $x^4 + y^4 = z^2$, $x^4 + y^4 = (z^2)^2$. Voici cette note, spécimen de ses démonstrations.

Si area trianguli esset quadratus, donantur duo quadrato-quadrati quorum differentia esset quadratus. Unde sequitur dari duo quadrata quorum et summa et differentia esset quadratus. Datur itaque numerus compositus ex quadrato et duplo quadrati æqualis quadrato, eā conditione ut quadrati eum componentes faciant quadratum. Sed si numerus quadratus compositur ex quadrato et duplo alterius quadrati, ejus latus similiter compositur ex quadrato et duplo quadrati, ut facillime possumus demonstrare. Unde concludatur latus illud esse summum laterum circa rectum trianguli rectanguli et unum ex quadratis illud componentibus efficere basem et duplum quadratum æquari perpendiculo.

Illud itaque triangulum rectangulum conficietur a duobus quadratis quorum summa et differentia erunt quadrati. At isti duo quadrati minores probabuntur primis quadratis suppositis quorum tam summa quam differentia faciunt

quadratum. Ergo si dantur duo quadrata quorum summa et differentia faciunt quadratum, dabitur in integris summa duorum quadratorum ejusdem naturæ priore minor. Eodem ratiocinio dabitur et minor ista inventa per viam prioris et semper in infinitum minores invenientur numeri in integris idem præstantes : quod impossibile est, quia dato numero quovis integro non possunt dari infiniti in integris illo minores.

Traduite dans les *Œuvres de Fermat,* t. III, par Tannery et Henry : « Si l'aire d'un triangle était un carré, il y aurait deux bicarrés dont la différence serait un carré ; il s'ensuit qu'on aurait également deux carrés dont la somme et la différence seraient des carrés. Par conséquent, on aurait un nombre carré, somme d'un carré et du double d'un carré, avec la condition que la somme des deux carrés qui servent à le composer soit également un carré. Mais, si un nombre carré est somme d'un carré et du double d'un carré, sa racine est également somme d'un carré et du double d'un carré, ce que je puis prouver sans difficulté.

« On conclura de là que cette racine est la somme des deux côtés de l'angle droit d'un triangle rectangle dont l'un des carrés composants formera la base et le double de l'autre carré la hauteur.

« Ce triangle rectangle sera donc formé par deux nombres carrés, dont la somme et la différence seront des carrés. Mais on prouvera que la somme de ces deux carrés est plus petite que celle des deux premiers, dont on a également supposé que la somme et la différence soient des carrés. Donc, si on trouve deux carrés dont la somme et la différence soient deux carrés, on donne par là même en nombres entiers deux carrés jouissant de la même propriété et dont la somme est inférieure.

« Par le même raisonnement, on aura ensuite une somme plus petite que celle déduite de la première et en continuant indéfiniment on trouvera toujours des nombres entiers de plus en plus petits, satisfaisant aux mêmes conditions. Mais

cela est impossible, puisque, un nombre entier étant donné, il ne peut y avoir une infinité de nombres entiers qui soient plus petits. »

§ II. $x^3 + y^3 = z^3$, par Euler.

Euler, né à Bâle en 1707, mourut en 1783.

Dans ses *Éléments d'Algèbre,* traduits de l'allemand par J. G. Garnier, professeur à l'Ecole Polytechnique, tome II, chap. xv, p. 260, 2[e] édition (1774) et p. 274, se trouve la *Résolution de quelques questions où l'on demande des cubes.*

Théorème. Il n'est pas possible de trouver deux cubes dont la somme ou la différence soit un cube.

Euler emploie la Descente infinie dans les deux cas considérés. Il s'exprime ainsi : On ne peut assigner, même parmi les grands nombres, deux cubes tels, et cela par la raison qu'on ne trouve point des cubes de cette espèce dans les plus petits nombres.

Démonstration de quatre pages in-8°.

Problème. On demande trois cubes dont la somme soit un cube.

Infinité de solutions avec deux arbitraires. Une page.

§ III. — Aire du triangle rectangle,

par Legendre (*Théorie des Nombres*, t. II, p. 1, 3[e] édition, 1830).

Legendre, né à Toulouse, en 1752, mourut en 1833.

Legendre cite le passage latin de Fermat dans ses *Observations sur Diophante,* au sujet de cette aire, et ajoute : « Nous le suivrons assez strictement, en ajoutant seulement les développements nécessaires pour rendre la démonstration plus claire et complète. »

Mais, tandis que Fermat avait gardé pour lui « le mystère de sa méthode », Legendre explique pour quelle raison, s'il y a un premier triangle, il y en a un second, et un second plus petit que le premier.

De plus, Legendre aboutit au théorème de Fermat pour $n = 4$.

§ IV. $x^3 + y^3 = z^3$, par Legendre.

Dans la *Théorie des Nombres*, t. II, p. 7, 3e édition, 1830, Legendre expose la démonstration d'Euler sans y rien changer ; seulement, il la complète, comme il avait complété celle de Fermat, en prouvant que les nouvelles indéterminées sont plus petites que les anciennes.

Dans ce même tome, p. 357, Legendre donnera une démonstration nouvelle, qui lui appartient.

§ V. $a^n = b^n + c^n$, par Abel.

Niels Henrik Abel, né à Findö, en 1802, mourut en 1829.

(*Œuvres d'Abel*, publiées par Holmboé, 1re édition ; la 2e a été publiée aux frais de l'État norvégien, Christiana, 1881.)

Extrait d'une lettre adressée par Abel à Holmboé :

« Copenhague, l'an $\sqrt[3]{6064321219}$, en comptant la fraction décimale,

24 juin 1823.

« ...J'ai cherché à démontrer l'impossibilité de l'équation $a^n = b^n + c^n$ en nombres entiers, lorsque n est plus grand que 2 ; mais je ne suis parvenu qu'aux théorèmes suivants, qui sont assez curieux... »

Suivent quatre théorèmes. Dans le 4e, Abel prend le cas de $n = 7$, et il trouve les plus petites valeurs que peuvent prendre a, b, c ; mais ces nombres ne satisfont pas à l'équation (1re édition) : 2438735, 2422355, 2360614.

§ VI. — Mémoire sur le théorème de Fermat, par Legendre.

Ce mémoire a paru dans les *Comptes rendus de l'Académie des Sciences* de Paris, t. VI, et dans la *Théorie des Nombres*, 1re et 3e éditions.

« ...Quoique l'Académie, en vue d'honorer la mémoire de Fermat, ait proposé pour sujet d'un de ses Prix de Mathématiques la démonstration de ce théorème, le concours, prorogé même au delà du terme ordinaire, n'a produit aucun résultat.

« Il semble donc qu'une difficulté particulière soit attachée à cette question et que nous manquions du principe spécial qui serait nécessaire pour la résoudre. En attendant qu'un hasard heureux fasse retrouver ce principe, tel que Fermat l'avait conçu, les amateurs de la Théorie des nombres verront peut-être avec plaisir que le cas des 5[èmes] puissances peut être démontré rigoureusement. »

Legendre commence par exposer quelques considérations générales sur les conditions auxquelles doivent satisfaire les inconnues :

« L'une de ces conditions est que n, ou même n^2, divise une inconnue. On remarquera que cette condition devient un problème difficile et non résolu dès que n dépasse 17. » Aussi Legendre a recours à une vérification s'étendant aux n plus petits que 100.

« Cette démonstration est due à M[lle] SOPHIE GERMAIN, qui a remporté le prix de l'Académie *Sur les vibrations des lames élastiques.* »

Legendre ajoute que la proposition s'étend jusqu'à 197 pour des n d'une certaine forme. En particulier, il prouve que si $x^5+y^5+z^5=0$ était possible, la plus grande des inconnues aurait au moins 153 chiffres et la plus petite 122.

Il passe enfin à la démonstration annoncée pour $n=5$. Il peut supposer que x, par exemple, est divisible par 5, mais il considère deux cas : x pair ou impair.

Il a recours à la descente infinie.

§ VII. $x^5+y^5+z^5=0$, par LEJEUNE-DIRICHLET.

LEJEUNE-DIRICHLET, né en 1805 à Düren, mourut en 1859 à Göttingue.

(*Journal de Crelle,* t. III, 1828). Mémoire lu par l'auteur le

14 juillet 1825 à l'Académie des Sciences de Paris et approuvé par les commissaires Lacroix et Legendre.

L'auteur démontre l'impossibilité des équations

$$x^5 \pm y^5 = 2^m 5^n A z^5$$

et en déduit le théorème de Fermat.

Il traite d'abord le cas de x pair et supposé divisible par 5.

« Il ne resterait que le cas de x impair ; mais la méthode exposée dans ce Mémoire paraît insuffisante dans ce cas et je ne sais pas comment on pourrait compléter la démonstration. »

Dans le même tome, p. 358, on lit : *Addition au Mémoire précédent.*

« Depuis que le Mémoire précédent a été présenté à l'Académie, M. Legendre a publié un second supplément à sa *Théorie des Nombres*, dans lequel il démontre l'impossibilité de l'équation $x^5 + y^5 = z^5$. Le cas de l'indéterminée divisible à la fois par 2 et par 5 est traité dans cet ouvrage comme dans le Mémoire précédent et l'auteur prouve ensuite l'impossibilité de l'autre cas au moyen d'une analyse nouvelle.

« L'objet de cette addition est d'établir deux théorèmes nouveaux sur les équations indéterminées du 5e degré, comprenant le théorème de Fermat. J'y parviens en partant des résultats obtenus dans ce qui précède et en y faisant usage d'une analyse qui diffère à plusieurs égards de celle de M. Legendre et entièrement analogue à la méthode exposée dans le Mémoire précédent. »

Remarque. — Lebesgue, professeur à la Faculté des Sciences de Bordeaux, donne une suite au Mémoire de Dirichlet en traitant l'équation $x^5 + y^5 = az^5$.

§ VIII. — Mémoire sur la théorie des nombres, par Libri (*Crelle*, t. IX, 1832).

« En général on pourrait démontrer que, étant donnée la congruence à deux inconnues $x^n + y^n + 1 \equiv 0 \pmod{p}$, on

pourra toujours assigner une limite de p telle que, pour cette limite, le nombre des solutions de cette congruence ira toujours en augmentant.

« Ce théorème n'est pas sans importance pour parvenir à la démonstration de l'impossibilité de résoudre l'équation $u^n + v^n = z^n$ en nombres entiers ; car il prouverait que l'on tenterait en vain de démontrer cette impossibilité en voulant établir que, si cette équation était résoluble, l'une des inconnues serait divisible par une infinité de nombres premiers. Nous faisons cette observation parce que nous avons des motifs de croire que plusieurs analystes ont tenté de faire cette démonstration. »

CHAPITRE III

DE LEGENDRE A LAMÉ

---

§ I. $x^{14}+y^{14}=z^{14}$,

par Lejeune-Dirichlet (*Journal de Crelle,* t. IX, p. 390, 1832).

L'auteur démontre l'impossibilité de cette équation en distinguant deux cas; dans celui où x est divisible par 14, il emploie la descente infinie.

§ II. $x^{2\lambda}+y^{2\lambda}=z^{2\lambda}$,

par Kummer, né en 1810, mort en 1893.
(*Journal de Crelle*, t. XVII, p. 203, 1837).

« ..... Les démonstrations particulières déjà données s'accordent en ceci que de l'équation proposée une autre équation de même forme est tirée, dont les inconnues sont plus petites que celles de la première: les artifices par lesquels les auteurs sont parvenus à cette équation *semblable* diffèrent beaucoup et ne permettent pas des applications à d'autres cas.

« Dans une question si difficile il nous semble nécessaire de commencer par les exposants pairs; bien que nous ne conduisions pas jusqu'au bout cette recherche plus facile, nous communiquons aux géomètres quelques résultats pouvant la faire avancer. »

Le Mémoire est écrit en latin. L'auteur s'appuie sur la formule d'Albert Girard. Il démontre seulement que, si l'équation était possible, l'équation $r^{2\lambda}+s^{2\lambda}=2q^{\lambda}$ le serait aussi, r, s, q diviseurs de y.

§ III. $x^7 + y^7 = z^7$,

par G. Lamé, né à Tours en 1795, décédé à Paris en 1870. (*Journal de Mathématiques pures et appliquées, de Liouville*, t. V, p. 195, 1840 et *C. R.*, t. IV, p. 359, 1839.)

« Je présente cette démonstration sans recourir à aucune théorie étrangère ; tous les lemmes nécessaires sont démontrés directement et uniquement en vue du nombre 7. »

Rapport de Cauchy; Liouville, commissaire. — « Les démonstrations d'Euler et de Legendre pour 3 et 5 fondées sur la théorie des formes quadratiques des nombres premiers et les difficultés que Legendre a eu à surmonter laissent peu d'espoir de les appliquer avec succès à d'autres cas. M. Lejeune-Dirichlet est parvenu, à l'aide d'un artifice de calcul, à le démontrer pour $n = 14$; M. Lamé, à son tour, pour $n = 7$.

« M. Lamé démontre un lemme:

$$\frac{x + y + z}{\sqrt[7]{(x + y)(y + z)(z + x)}}$$

est un carré parfait.

« A l'aide de ce lemme, il prouve qu'il est impossible de supposer les trois inconnues non divisibles par 7, ce qu'on savait déjà. Ensuite, en s'appuyant sur le lemme et en supposant une inconnue divisible par 7, il remplace l'équation proposée du 7ᵉ degré par une équation telle que $z^4 = x^8 - 3x^4y^4 + \frac{16}{7}y^8$; et il démontre l'impossibilité de résoudre cette dernière à l'aide d'une suite d'équations semblables.

« En lisant avec soin le Mémoire de M. Lamé, nous nous sommes demandé : 1° si le lemme se trouve compris dans quelque autre proposition plus générale, relative à une valeur quelconque de n ; 2° s'il ne serait pas possible d'abréger encore la démonstration.

« Nous avons reconnu, en effet, que le lemme est une conséquence de cette proposition :

« *Si l'on retranche la somme des puissances* $n^{ièmes}$ *de deux inconnues* x, y *de la puissance* $n^{ième}$ *de leur somme, le reste sera divisible algébriquement non seulement par le produit* $nxy(x+y)$, *mais encore, pour des valeurs de* n *plus grandes que* 3, *par le trinome* x^2+xy+y^2 *et même par son carré si* $n=6k+1$.

« Nous avons aussi reconnu qu'on abrège la démonstration quand on commence par établir l'impossibilité de résoudre l'équation $z^2=x^4-\frac{3}{4}x^2y^2+\frac{1}{7}y^4$, y étant pair.

« En résumé, les commissaires pensent que le manuscrit de M. Lamé est digne de l'approbation de l'Académie et mérite d'être inséré dans le *Recueil des Savants étrangers.* »

§ IV. $x^7+y^7=z^7$,

par LEBESGUE, professeur à Bordeaux. (*Journal de Liouville,* t. V, p. 184, 1840.)

L'auteur se propose de simplifier la démonstration de Lamé. Il ne distingue pas deux cas, et, comme l'avait suggéré Cauchy, il part d'une équation $z^2=x^4-Ax^2y^2+By^4$.

Une omission lui ayant été signalée par Lamé, il compléta sa démonstration.

§ V. $x^{2n}+y^{2n}=z^2$,

par LEBESGUE, *Journal de Liouville,* t. V. p. 184, 1840).

THÉORÈME. — *Si* $t^n+v^n=w^n$ *est possible, il en sera de même de* $x^{2n}+y^{2n}=z^2$.

§ VI. $z^{2n}-y^{2n}=2x^n$,

par LIOUVILLE, né à Saint-Omer en 1809, mort en 1882. (*Journal de Liouville,* t. V, p. 360, 1840.)

THÉORÈME. — *L'impossibilité de* $t^{2n}+v^{2n}=w^2$ *entraîne celle de* $z^{2n}-y^{2n}=2x^n$.

§ VII. — Binomes cubiques $X^3 + Y^3$,

par Lamé (*C. R.*, n° 61, p. 921, 1865 et *Journal de Liouville*).

L'auteur étudie les propriétés, les relations et les valeurs des binomes cubiques. Il démontre que tout nombre entier est la valeur commune d'une suite infinie de rapports dont les deux termes sont des binomes cubiques ; si cet entier est un cube, le problème d'Euler, *Trouver quatre cubes dont la somme algébrique soit nulle* se trouvera résolu.

CHAPITRE IV

DE LAMÉ A KUMMER

§ I. — **Lettre de Kummer à Liouville**
(*Journal de Liouville,* t. XII, p. 136).

« Breslau, 28 avril 1847.

« Engagé par mon ami, M. Lejeune-Dirichlet, je prends la liberté de vous envoyer quelques exemplaires d'une dissertation que j'ai écrite il y a trois ans à l'occasion du jubilé séculaire de l'Université de Kœnigsberg et d'une autre démonstration d'un de mes amis et disciples, M. Kronecker.

« Dans ces Mémoires vous trouverez des développements sur quelques points de la théorie des nombres complexes, qui ont été récemment le sujet de quelques discussions au sein de votre illustre Académie à l'occasion de l'essai d'une démonstration du théorème de Fermat, proposé par M. Lamé.

« Quant à la proposition élémentaire, pour ces nombres complexes, qu'un nombre complexe composé ne peut être décomposé en facteurs premiers que d'une seule manière, que vous regrettez très justement dans cette démonstration, défectueuse en outre en quelques autres points, je puis vous assurer qu'elle n'a pas lieu généralement, tant qu'il s'agit des nombres complexes de la forme $\alpha_0 + \alpha_1 r + \cdots + \alpha_{n-1} r^{n-1}$, mais qu'on peut la sauver en introduisant un nouveau genre de nombres complexes que j'ai nommé nombre complexe *Idéal.*

« Les résultats de mes recherches ont été communiqués à l'Académie de Berlin et imprimés dans les Comptes rendus

pour 1846. Un Mémoire sur le même sujet paraîtra bientôt dans le *Journal de Crelle*.

« Les applications de cette théorie à la démonstration du théorème de Fermat m'ont occupé depuis longtemps et j'ai réussi à faire dépendre l'impossibilité de l'équation

$$x^n + y^n = z^n$$

de deux propriétés du nombre premier n, en sorte qu'il ne reste plus qu'à rechercher si elles appartiennent à tous les nombres premiers ... »

Note de Liouville. — « Le Mémoire de M. Kummer (1844) est écrit en latin sous le titre *De numeris complexis qui radicibus unitatis et numeris integris realibus constant.*

« Celui de M. Kronecker est intitulé *De unitatibus complexis* (1846).

« Le Mémoire de M. Kummer offre beaucoup d'intérêt,..

« Nous n'avons pas à examiner en quoi les auteurs cités s'accordent ou diffèrent. C'est au temps de fixer la valeur de leurs travaux. »

§ II. — Mémoires sur les nombres complexes, par Lamé (*C. R.*, t. XXIV, 1847).

Séance du 1er mars, p. 310. *Communication de Lamé.* « On possède des démonstrations pour 3, 5, 7, fondées sur la décomposition du premier membre de l'équation en deux facteurs. Mais avec 11, 13, 17, 19... on est arrêté par la trop grande inégalité des deux facteurs.

« Je cherchais depuis longtemps un genre de démonstration applicable à tous les cas, lorsque, il y a quelques mois, j'en causais avec M. Liouville. Il parut convaincu que la proposition négative énoncée par Fermat devait dépendre de certains facteurs complexes, récemment étudiés par les géomètres qui s'occupent de la Théorie des nombres. C'était une nouvelle voie, que je n'avais pas explorée et que j'ai suivie. » Suit le premier Mémoire.

Observations de Liouville : « L'idée d'introduire des N. C. (nombres complexes) dans la théorie de l'équation $x^n - y^n = z^n$ n'a rien de nouveau et a dû se présenter naturellement aux géomètres d'après la forme binaire $x^n - y^n$. Je n'en ai d'ailleurs déduit aucune démonstration satisfaisante. Toutefois, quelques essais me portaient à croire qu'il faudrait d'abord chercher à établir pour les N. C. un théorème analogue à la proposition élémentaire pour les nombres entiers, qu'un produit ne peut être décomposé en facteurs premiers que d'une seule manière.

« L'analyse de M. Lamé me confirme dans cette opinion. N'y a-t-il pas là une lacune à remplir?

« Je rappellerai, en terminant, que, depuis M. Gauss e même depuis Euler et Legendre, les géomètres se sont occupés des N. C. Le tome XVII de nos Mémoires renferme un grand travail de M. Cauchy où ceux de ces nombres qui se rattachent à l'équation $x^n - 1 = 0$ jouent un rôle important, et c'est surtout dans un article de M. Jacobi (*Journal de Mathématiques*, t. VII, p. 268) qu'on trouve d'utiles renseignements. »

Intervention de Cauchy. Il rappelle un Mémoire, présenté à l'Académie le 19 octobre 1846, dans lequel il exposait une méthode et des formules devant pouvoir servir à la démonstration du théorème de Fermat. Mais cette méthode diffère de celle de M. Lamé.

Séance du 8 mars, p. 352. *Note de Lamé.* « ... La définition et les caractères principaux des N. C. sont sans doute insuffisants, si l'on ne prouve pas qu'ils jouissent des propriétés de divisibilité qui appartiennent aux nombres entiers et si l'on ne se met pas à l'abri de l'embarras provenant des facteurs qui, comme r et $r + \frac{1}{r}$, se présentent dans la décomposition du nombre *un*. Sous ce point de vue, il existe évidemment une lacune dans ma communication, mais je ne tarderai pas à la combler. »

Séance du 22 mars, p. 921. *Note de Cauchy*. Il confirme l'observation de M. Liouville et signale un autre point douteux dans le théorème de Lamé : les expressions désignées par z_i. En effet, z_i étant, comme l'a remarqué encore M. Liouville, un diviseur de l'unité, on ne saurait dire que ses puissances ne peuvent diviser certains nombres complexes.

Séance du 5 avril, page 569. « Ce Mémoire a pour but de rectifier et de compléter le mode de démonstration générale présenté le 1er mars. L'erreur concernait les facteurs imaginaires dont le module est l'unité.

« Obligeamment averti par M. Liouville, j'ai repris une partie de mon Mémoire.

« Pour plus de clarté, je suppose $n = 5$. »

Séance du 24 mai, page 888. Dans un troisième Mémoire, Lamé étend à beaucoup d'autres nombres la démonstration appliquée à l'exposant 5.

§ III. — Mémoires de Cauchy

(*C. R.*, 1839, 1847).

L'auteur étudie exclusivement les nombres complexes ; le nom du théorème de Fermat ne figure que dans les titres de ces mémoires. Dans le dernier seulement, il énonce, sans démonstration, comme conséquence de ses recherches, une condition suffisante, dans le cas où x, y, z sont premiers à n, pour que l'équation n'ait pas lieu. Cette condition est purement arithmétique.

§ IV. — Théorie des nombres complexes et Application au théorème de Fermat,

par Kummer.

Daté de Breslau (1849), ce mémoire a été publié dans le *Journal de Crelle*, t. XX, p. 130, 1850, et le *Journal de Liouville*, t. XVI, p. 377, 1851.

Il contient la définition et les propriétés générales des facteurs *idéaux* d'un N. C. (nombre complexe), la composition des N. C. idéaux, la recherche du nombre de classes des N. C. idéaux, la définition d'un facteur premier idéal d'un nombre entier et l'étude des unités complexes.

« ... Dans tout ce qui précède, la théorie des N. C. est avancée à un point où la démonstration du théorème de Fermat se fait avec facilité, si l'exposant λ n'est compris, comme facteur du numérateur, dans aucun des $\frac{\lambda - 3}{2}$ premiers nombres bernoulliens. Dans la première centaine, 37, 59, 67, seuls, échappent à la démonstration, parce qu'ils divisent respectivement les 16e, 22e, 29e nombres bernoulliens.

« Comme la démonstration pour les N. C. est aussi facile que pour les nombres entiers non complexes, nous supposerons que, dans l'équation $u^\lambda + v^\lambda + w^\lambda = 0$, u, v, w sont des N. C. »

A l'appui de sa conception du N. C. idéal, l'auteur écrit :

« L'algèbre, l'arithmétique et la géométrie offrent de nombreuses analogies avec notre théorie. On décompose, par exemple, les fonctions rationnelles et entières d'une variable en facteurs linéaires, quoique ces facteurs isolés n'existent que dans des cas particuliers ; c'est pour ce but qu'on a créé les quantités imaginaires.

« En géométrie, on parle d'une droite passant par les points d'intersection de deux cercles, quand même ces points n'existent pas. Dans cet exemple, la propriété permanente que les tangentes menées d'un point quelconque de cette ligne aux deux cercles sont égales entre elles est l'analogue de la propriété des N. C. $f(x) = 0$ (mod. q) pour $\eta = u_r$, et la propriété accidentelle de cette ligne de passer par les points d'intersection des deux cercles est, de même, analogue à la propriété accidentelle des N. C. $f(x)$ d'avoir un facteur premier existant $\varphi(\eta)$.

« La composition des N. C. peut être envisagée comme

l'analogue de la composition chimique, les facteurs premiers correspondant aux équivalents des éléments. Les N. C. idéaux sont comparables aux radicaux hypothétiques qui n'existent pas par eux-mêmes, mais seulement dans les combinaisons ; le fluor, en particulier, comme élément qu'on ne sait pas représenter isolément, peut être comparé à un facteur premier idéal.

« La notion de l'équivalence des nombres idéaux est, au fond, la même que celle de l'équivalence chimique ; car, ainsi que des quantités pondérales peuvent être substituées les unes aux autres pour rendre des sels neutres ou des corps isomorphes, de même les nombres idéaux, remplacés par les facteurs équivalents, ne produisent que des nombres idéaux de la même classe.

« Enfin, de même que les réactifs chimiques, joints à un corps en dissolution, donnent des précipités au moyen desquels on reconnaît les éléments contenus dans le corps proposé, de même les nombres que nous avons désignés par $\psi(\eta)$, comme réactifs des N. C., font connaître les facteurs premiers contenus dans les N. C., en mettant en évidence un facteur premier q, analogue au précipité chimique. »

§ V. — Démonstration d'un théorème de Kummer,

par Léopold Kronecker (*J. de Liouville,* t. I, p. 396, 1856).

L'auteur démontre simplement, à l'aide de congruences, le théorème visant les $\frac{\lambda - 3}{2}$ premiers nombres bernoulliens.

§ VI. — Sur les équations cubiques à coefficients rationnels,

par Kronecker (*J. de Crelle,* 1859).

L'auteur démontre l'impossibilité de $r^3 + s^3 = 1$, r et s étant remplacés par $\frac{2a}{3b - 1}$, $\frac{3b + 1}{3b - 1}$.

§ VII. — Grand prix de Mathématiques.

L'Académie des Sciences de Paris a proposé, comme sujet du prix de mathématiques, la démonstration du théorème de Fermat, une première fois en 1823, une seconde fois en 1850 (C. R., t. XXIX et t. XXX, 1843).

En 1823, le concours fut même prorogé (Legendre, § 6).

En 1850 : trouver pour un exposant entier quelconque les solutions en nombres entiers de l'équation $x^n + y^n = z^n$, ou prouver qu'elle n'en a pas. Commissaires : Cauchy, Sturm, Arago, Poinsot; Liouville, rapporteur.

Le prix consistera en une médaille d'or, de la valeur de 3 000 francs.

Cinq mémoires ont été envoyés, aucun d'eux n'a été jugé digne du prix. Les commissaires sont d'avis que la même question soit remise au concours pour l'année 1858, et dans les mêmes termes (C. R., janvier 1854) ; commissaires : Sturm, Liouville, Lamé, Poinsot ; Cauchy, rapporteur.

Dix-huit mémoires ont été envoyés, quelques-uns renfermaient d'ingénieuses tentatives.

Enfin, dans sa séance du 9 février 1857, le dernier mot fut dit ; commissaires : Liouville, Lamé, Chasles ; Cauchy, rapporteur.

« Onze mémoires ; mais aucun d'eux n'a résolu la question. Seulement, les commissaires ont remarqué dans la pièce inscrite au numéro 2 une solution nouvelle du problème dans le cas spécial, développé par Fermat lui-même, où l'exposant est 4.

« Ainsi, après avoir été plusieurs fois remise au concours, la question en est restée au point où l'a laissée M. Kummer. Toutefois, les sciences mathématiques n'ont qu'à se féliciter des travaux que le désir de la résoudre a fait entreprendre aux géomètres, spécialement à M. Kummer, et les commissaires pensent que l'Académie prendrait une détermination utile et honorable si, en retirant la question du concours,

elle adjugeait la médaille à M. Kummer pour ses belles recherches sur les nombres complexes, composés des racines de l'unité et des nombres entiers. » Ces propositions ont été adoptées.

Le problème a été mis également au concours par l'Académie de Bruxelles.

CHAPITRE V

DE KUMMER A MIRIMANOFF

§ I. — Mélanges mathématiques transcendants,

par F. Landry. Librairie Hachette. — Bachelier, éditeur (1853).

Le premier des six Mémoires rappelle ce principe de Legendre :

Pour chaque valeur du nombre n premier, il existe un nombre premier θ, ou $2kn+1$, tel qu'on ne peut pas satisfaire à l'égalité $r'=r+1$, r, r' étant deux résidus de puissances $n^{\text{ièmes}}$, divisées par θ, et tel, en même temps, que n ne soit pas un de ces résidus.

« Legendre démontre ensuite que cette double condition est satisfaite par $2n+1$, toutes les fois que $2n+1$ est premier et qu'il en est de même pour les nombres premiers de la forme $4n+1$, $8n+1$, $16n+1$; puis, il ajoute que l'on vérifierait de la même manière que les deux conditions sont encore remplies pour les cas de $\theta=10n+1$, $\theta=14n+1$, mais il ne fait pas cette vérification.

Pour ne laisser aucune incertitude sur cette matière délicate, en dehors de l'autorité du maître (αυτος εφη), nous essayons de combler cette lacune. »

Dans le second Mémoire, l'auteur montre que l'impossibilité de la relation $a^n+b^n=c^n$ se rattache à l'impossibilité de certaines relations de la forme $\alpha^x+\alpha^y+\alpha^z=0$, α étant une des racines primitives de $x^{2k}\equiv 1$, relativement à un facteur premier θ de la forme $2kn+1$.

§ II. — Extension du théorème de Fermat,

par A. Genocchi (*C. R.*, t. LXXXII, p. 910, 1876).

« Il est impossible de satisfaire à l'équation

$$x^7 + y^7 + z^7 = 0,$$

en prenant pour x, y, z les racines d'une équation du 3ᵉ degré à coefficients rationnels, et cela résulte de l'impossibilité de résoudre en nombres entiers l'équation

$$z^2 = x^4 + 6x^2y^2 - 4y^4. \text{ »}$$

L'auteur emploie la descente infinie.

§ III. $X^n + Y^n + Z^n = 0$, par Liouville

(*C. R.*, t. LXXXVII, 1879).

L'auteur démontre, en partant de l'intégrale

$$\int \frac{\alpha^{n-1} d\alpha}{(1 - \alpha^n)^{\frac{1}{n}}},$$

où $\alpha = \frac{Y}{Z}$, que l'équation de Fermat n'est pas satisfaite par des polynomes, rationnels et entiers, de degré quelconque, à une variable.

§ IV. $X^n + Y^n + Z^n = 0$, par Korkine

(*C. R.*, t. XC, 1880).

Extrait d'une lettre de l'auteur à Hermite : « M. Liouville vient de donner une démonstration de l'impossibilité de l'équation $X^n + Y^n + Z^n = 0$ par des polynomes X, Y, Z, que je modifie par des considérations de degrés. »

§ V. — **Sur un théorème de Fermat,**

par Th. Pépin, S. J. (*Atti dell' Academia pontificia del Nuovi Lincei*, t. XXXVI, p. 23, 1882).

L'auteur signale une lettre de Fermat à Frénicle, dans laquelle Fermat affirme que 7 est le seul nombre jouissant de cette propriété : un nombre égal à deux fois un carré, moins l'unité, et égal à la racine carrée d'un nombre de même nature : $7 = 2 . 2^2 - 1 = \sqrt{2 . 5^2 - 1}$.

Il semble dire que cette proposition n'a jamais été établie ; et il finit ainsi : si un autre nombre que 7 existe, il est supérieur à l'unité suivie de 3 848 chiffres, de sorte qu'on ne pourra jamais trouver un nombre donnant un démenti à l'assertion de Fermat.

§ VI. — **Sur le dernier théorème de Fermat,**

par E. de Jonquières (*Atti dell' Academia pontificia del Nuovi Lincei*, 1884, et *C. R.*, t. XCVIII, p. 863, 1884).

Dans les Atti : « En attendant la démonstration complète, on peut démontrer, et même de la façon la plus élémentaire, l'exactitude de l'affirmation de Fermat dans l'un des trois cas généraux qui comprennent, ensemble, tout l'énoncé de la proposition.

« En effet, de trois choses l'une : 1° les nombres mineurs a, b premiers ; 2° a ou b premier, l'autre composé ; 3° a et b composés.

« Au premier cas appartient la démonstration qu'on va lire ; elle fait aussi connaître deux conditions auxquelles b et c sont assujettis dans le second cas. »

Dans les C. R. L'auteur résume les théorèmes contenus dans la Note : la somme des puissances $n^{\text{ièmes}}$ de deux nombres premiers n'est jamais égale à une puissance $n^{\text{ième}}$. — Si $n = 2$ et l'équation satisfaite, c'est toujours a, si $a < b$, qui est premier. — La différence des puissances $n^{\text{ièmes}}$ de deux

entiers consécutifs n'est jamais la puissance $n^{ième}$ d'un nombre premier.

« C'est dans le même ordre d'idées que Abel paraît avoir étudié la question. »

§ VII. — **Sur le dernier théorème de Fermat,**

par C. CATALAN (*Bulletin de l'Académie royale des Sciences, lettres et Arts de Belgique*, 56[e] année, 3[e] série, t. XII, p. 498, 1886).

« En suivant la voie indiquée par M. de Jonquières, on peut trouver d'autres contributions au théorème de Fermat. Afin de prendre date, j'énoncerai les propriétés suivantes... »

Catalan est mort en 1895. Le *Bulletin* ne contient, de 1886 à 1895, aucun nouvel article de lui.

§ VIII. — **Sur le dernier théorème de Fermat,**

par MANSION (*Même Bulletin*, t. III, p. 16 et 125, 1887).

L'auteur, sans faire allusion à l'article de Catalan, démontre que x et z sont composés.

§ IX. — **Note en connexion avec le théorème de Fermat,**

par G. B. MATHEWS (*Messenger of Mathematics*, vol. XX, p. 68, 1885-6).

« ... La méthode de Kummer, par les moyens de sa théorie du nombre premier idéal, est décidément compliquée... »

La note suivante fait usage des congruences ordinaires. L'auteur démontre que x, y ou z doit être divisible par n, pour $n = 3, 5, 11, 17$. « Mais, quand même $n = 7$, j'ai été incapable de quelque progrès digne de mention. »

§ X. — Sur une question de la théorie des nombres,

par D. Mirimanoff, à Genève (*Journal de Crelle*, n° 31, 108-109, p. 82, 1891).

M. D. Mirimanoff est né à Périaslavl (Russie) le 13 septembre 1861.

« Soit θ une racine primitive de $x^\lambda = 1$; λ premier ; H le nombre de classes des nombres idéaux formés avec θ ; a le premier facteur et $\frac{H}{a} = b$ le second facteur de H (Kummer, *J. de Crelle*, t. XL, p. 113).

« Je suppose que H soit divisible par λ ; dans ce cas, λ divise a. Quant à b, il peut ne pas être divisible par λ. M. Kummer a fait voir, en effet, que b ne contient pas λ pour $\lambda = 37$, 59, 67, qui sont les seules valeurs de λ inférieures à 100 telles que $a \equiv 0$ (mod. λ) (*Abhandlungen der Berliner Akademie*).

« Je vais donner un nouveau criterium de la divisibilité de b par λ. »

L'auteur finit par le cas de $\lambda = 37$ et démontre que b n'est pas divisible par 37.

§ XI. — Sur l'équation $x^{37} + y^{37} = z^{37}$,

par D. Mirimanoff, à Genève (*Journal de Crelle*, t. CVIII, p. 26, 1893).

« M. Kummer a prouvé (*Crelle*, t. XL) que

$$x^\lambda + y + z^\lambda = 0$$

est impossible si H n'est pas divisible par λ. Il s'est occupé ensuite du cas de $H \equiv 0$ (mod. λ) et est parvenu à étendre son théorème à un groupe de ces λ (*Abhandlungen der Berliner Akademie*, 1857).

« Ce groupe comprend 37, 59, 67, pour lesquels $H \equiv 0$ (mod. λ).

« Je ferai voir que les propriétés des unités complexes que j'ai établies dans mon précédent Mémoire (*Crelle*, t. CVIII-

CIX, p. 82, 1892) suffisent pour démontrer le théorème de M. Kummer dans le cas particulier de $\lambda = 37$. »

§ XII. — **Des nombres complexes, d'après Kummer,**

par H. J. S. Smith, professeur à Oxford — *The collected mathematical Papers,* édité par Glaisher, professeur à Cambridge (1894-5).

L'auteur fait en note l'historique des diverses démonstrations. Il dit : « Cauchy essaie de prouver une proposition, fausse pour les N. C. considérés, à savoir que la norme du reste, dans la division d'un N. C. par un autre, peut être rendue moindre que celle du diviseur. Ailleurs, il prend la proposition comme une hypothèse et en déduit des conclusions fausses. Mais, plus loin, il reconnaît et corrige ces inexactitudes (*C. R.*, t. XXIV).

« Les résultats auxquels il arrive dans ses mémoires suivants sont en grande partie compris dans la théorie générale de Kummer. A un endroit cependant, il énonce sans démonstration l'important résultat suivant : *Si l'équation* $x^\lambda + y^\lambda + z^\lambda = 0$ *est résoluble*, x, y, z *dénotant des nombres premiers à* λ, *la somme* $1 + 2^{\lambda-4} + 3^{\lambda-4} + \ldots + \left(\frac{\lambda-1}{2}\right)^{\lambda-4}$ *est divisible par* λ. (Comparer le mémoire de Kummer dans les *Berliner Transactions*, p. 64, 1857.) »

C'est des travaux de Kummer que l'auteur s'occupe principalement. « L'impossibilité a été démontrée par Kummer, d'abord pour toutes les valeurs de λ non comprises dans les nombres premiers non exceptionnels (*Liouville*, t. XVI et *Crelle*, t. XI) et ensuite pour tous les nombres premiers exceptionnels qui satisfont aux trois conditions suivantes :

1° Que le premier facteur de H, quoique divisible par λ, ne le soit pas par λ^2 ;

2° Qu'un module complexe peut être assigné pour lequel une certaine unité complexe n'est pas congrue à une $\lambda^{ième}$ puissance ;

3° Que B_K n'est pas divisible par λ^3, B_K représentant le nombre bernoullien ($K \leqslant \mu - 1$) qui est divisible par λ (*Mémoires de l'Académie de Berlin,* 1857).

« Trois nombres, au-dessous de 100, 37, 59, 67, sont des nombres premiers exceptionnels. Mais il a été établi par Kummer que les trois conditions données sont satisfaites dans le cas de ces trois nombres, de sorte que l'impossibilité de l'équation de Fermat a été démontrée pour toutes les valeurs de l'exposant au-dessous de 100. En vérité, il serait probablement difficile de trouver un nombre premier exceptionnel ne satisfaisant pas aux trois conditions, et, par conséquent, exclu de la démonstration de Kummer. »

Quand Smith arrive à la représentation des nombres idéaux comme racines des nombres actuels, il dit : un nombre idéal ne peut être exhibé dans une forme isolée comme un entier complexe ; il n'a pas une existence quantitative, et l'assertion qu'un N. C. donné contient un facteur idéal est seulement une manière conventionnelle d'exprimer un certain nombre de conditions congruentielles qui sont satisfaites par les coefficients du nombre complexe. La représentation symbolique $f(\alpha)$, $F(\alpha)$, $\varphi(\alpha)$ des nombres idéaux est une véritable convention et tend à abréger de nombreuses démonstrations. »

§ XIII. $x^n + y^n = z^n$, par M. G. Korneck,

professeur au gymnase de Kempen (Posen) (*Archiv der Mathematik und Physik,* t. XIII, p. 1, 1895).

Rapport verbal concernant la démonstration adressée par M. Korneck à l'Académie des Sciences de Paris ; commissaires : Picard, Poincaré, rapporteur (*C. R.*, t. CXVIII, p. 84, 1894).

L'auteur établit un lemme en partant d'une équation $nx^2 + ky^2 = z^n$, et il parvient à donner cette forme à $x^n + y^n = z^n$, dont il démontre l'impossibilité, n impair.

Si $n = 2^m$, il traite l'équation $x^4 + y^4 = z^4$ sans se servir du lemme.

Plus tard, averti d'une erreur pour le cas de $n=3$, il corrige.

§ XIV. — **Note en connexion avec le théorème de Fermat,**

par G. B. Mathews (*The Messenger of Mathematics*, t. XXIV, p. 97, 1895).

L'auteur part de l'équation $x^k=1$ et du produit formé des facteurs, sommes de trois racines associées de toutes les manières possibles. Ce produit est égal à $\pm u_k^k$, k non multiple de 3 et u entier positif.

Il applique les résultats trouvés à l'équation

$$x^p+y^p+z^p=0$$

et conclut ainsi : « Si on pouvait montrer que, lorsque p est donné, il y a une infinité de nombres premiers $kp+1$, pour lesquels la congruence $u_k \equiv 0 \pmod{kp+1}$ n'est pas satisfaite, le théorème de Fermat serait démontré.

Une autre possibilité est que le plus grand facteur premier de u_k ne surpasse pas $2k+1$; cela encore, si c'était vrai, pourrait prouver le théorème. »

§ XV. — **Sur l'équation** $ax^{\lambda^t}+by^{\lambda^t}=cz^{\lambda^t}$,

par Edmond Maillet, professeur à l'École des Ponts et Chaussées (*Association française pour l'Avancement des Sciences*, 2[e] partie, p. 156, 1897).

« L'étude de l'équation a donné lieu à de nombreux travaux ; les plus remarquables, relatifs à $t=a=b=c=1$, sont ceux de Sophie Germain, Legendre, Cauchy et Kummer. Sophie Germain a établi l'impossibilité dans le cas où x, y, z sont premiers à λ, pour $\lambda<100$; Legendre pour $\lambda<197$.

« D'autres études ne supposent pas a, b, c égaux à 1.

« Nous nous proposons d'appliquer une des méthodes très simples indiquées par Legendre et d'établir l'impossibilité de l'équation pour une foule de valeurs de a, b, c, λ. Nous éten-

drons ensuite les résultats de Sophie Germain et de Legendre au cas de $\lambda < 223$, en supposant x, y, z premiers à λ, ainsi que a, b, c. »

L'auteur établit ensuite que si λ^{t-1} est la plus haute puissance du nombre premier λ qui divise H, l'équation est impossible en nombres entiers complexes.

Il étudiera $x^\lambda + y^\lambda = cz^\lambda$, où λ est < 100 et non exceptionnel (*Acta mathematica*, t. XXIV, p. 247, 1901, et *C. R.*, t. CXL, p. 1229, 1905).

§ XVI. — Memoria bibliografica dell' ultimo teorema di Fermat,

par Dionisio Gambioli (*Periodico di Matematica per l'insegnamento secondario*, série 2, t. XVI, p. 145, 1901).

« Ce mémoire a pour but de mettre sous les yeux des géomètres tous les mémoires concernant ce théorème, qui ont vu le jour, et, entre autres, une démonstration générale du Professeur Calzolari de Ferrare, démonstration pour laquelle me vient un doute au sujet de sa véracité.

« Les démonstrations particulières déjà trouvées paraissent d'autant plus compliquées et artificielles, quand on les compare à quelques-unes données par Fermat, qui brillent par la clarté. la simplicité, la brièveté, l'élégance. Leurs auteurs n'ont probablement pas pris le bon chemin. et, leur imagination augmentant la difficulté de la démonstration, ils ont voulu inventer des méthodes compliquées, qui, au lieu de conduire à la démonstration désirée, les en ont de plus en plus éloignés.

« Admettons que Fermat ait trouvé une démonstration simple et rigoureuse de son dernier théorème, comme il l'a assuré ; et, certainement, dans cette démonstration il n'a employé que des nombres réels ; aussi, il me semble que vouloir employer à ce sujet d'autres nombres pour faire une démonstration beaucoup plus générale que son théorème, c'est vouloir compliquer la question. »

L'auteur transcrit ensuite en partie les articles, au nombre de dix, d'Euler, Lagrange, Lejeune-Dirichlet, Lamé, Cauchy, Liouville, Kummer.

Il démontre le théorème de Fermat pour $n = 4$, $n = 5$ et exprime pour $n = 2$ les valeurs des inconnues en fonction de deux paramètres.

Quant à Calzolari, il exprime en fonction de trois paramètres les inconnues pour $n = 3$ et pour n quelconque, et en déduit l'impossibilité de ces équations.

A son mémoire bibliographique, Gambioli ajoute dans le tome suivant, t. XVII, un appendice relatif aux articles de Lamé et de Cauchy et à l'intervention de Kummer. Il en conclut que « ces articles ont suggéré au professeur de Berlin son mémoire et lui ont indiqué le chemin qu'il a pu suivre ». Daté de Milan, mars 1901.

§ XVII. — **Le critérium de Kummer,**

par D. Mirimanoff (*Journal de Crelle,* t. CXXVIII, p. 45, 1905).

« Aucune démonstration ne s'applique à tous les exposants. Parmi les méthodes employées, les plus belles sont certainement celles de Kummer. Celle de 1857 pour les nombres exceptionnels n'a peut-être pas été remarquée. Je voudrais rappeler le résultat principal obtenu par Kummer. J'essaierai de le réduire à sa plus simple expression.

« Je me servirai de polynomes déjà étudiés par Euler et aussi d'une méthode ingénieuse, due à Sophie Germain et à Legendre et reprise récemment par M. Ed. Maillet. »

§ XVIII. — **Intermédiaire des Mathématiciens.**

Notice bibliographique sur le théorème de Fermat (1905).

M. Edmond Maillet ajoute à la notice le mémoire de Legendre (C. R., t. VI, 1823), qui avait été oublié. « Cependant dans ce Mémoire, dont la lecture est facile, Sophie Germain et Legendre obtiennent, dans le cas où x, y, z sont

réels et premiers à n, des résultats plus étendus que ceux trouvés plus tard par Kummer. Jusqu'ici leur méthode est la plus simple et la plus puissante pour ce cas. »

§ XIX. — Sur l'équation diophantienne $x^3y + y^3z + z^3x = 0$ et sur $x^7 + y^7 + z^7 = 0$,

par HURWITZ, à Zurich (*Mathematische Annalen*, t. LXV, p. 228, 1908).

« Dans la théorie de la transformation du septième ordre des fonctions elliptiques, on sait que la courbe

$$x^3y + y^3z + z^3x = 0,$$

qui possède 168 collinéations, joue un rôle considérable (Mêmes *Annales*, t. XIV, p. 428). »

Cette courbe n'a pas de point à coordonnées entières, non nulles. L'auteur en déduit l'impossibilité de l'équation

$$x^7 + y^7 + z^7 = 0.$$

§ XX. — Sur le dernier théorème de Fermat,

par le professeur L. E. DICKSON. *Premier mémoire : Messenger of Mathematics*, vol. XXXVIII, p. 14, 1908 ; *Second mémoire : Quarterly Journal*, t. LX, p. 27, 1909).

« Sans aucun doute, le plus important travail fait à son sujet est celui de Kummer, dont la démonstration s'applique à une classe étendue de nombres premiers n ; mais il est très pénible de s'assurer si un n tombe ou ne tombe pas dans la classe de Kummer.

« Tous les auteurs ont jugé nécessaire de séparer deux cas. Dans le premier, une méthode très simple a été inventée par Sophie Germain et généralisée par Legendre, applicable à tout nombre premier n, pour lequel un des nombres $mn + 1$, où $m = 2, 4, 8, 10, 14, 16$ est premier (le cas exceptionnel de $n = 3$, pour $m = 10$ et 14, étant mis de côté).

« Dans le présent mémoire (le premier), j'obtiens ce résultat

par une analyse générale, directe, et je l'étends aux nouvelles classes, $m = 20, 22, 26, 28, 32, 40, 56, 64$ (les valeurs exceptionnelles de n étant données à part). Sophie Germain a prouvé l'impossibilité de $u^n + v^n + w^n = 0$ pour chaque impair, premier, < 100 ; Legendre, pour $n < 200$; Maillet, pour $n < 223$; Mirimanoff, pour $n < 257$. Je la prouve pour $n < 1700$. »

Dans le second mémoire, il la prouve pour $n < 6857$.

§ XXI. — **Prix Wolfskehl** (1908).

En vertu des pouvoirs que nous a donnés M. le docteur Paul Wolfskehl, décédé à Darmstadt, nous fondons par les présentes un prix de cent mille marks, sous le nom de Ein hunderttausend mark, qui sera délivré à celui qui donnera le premier une démonstration du grand théorème de Fermat.

Dans un testament, M. le docteur Wolfskehl observe que Fermat (*Œuvres*, Paris, 1891, t. I, p. 291, Obs. 2) affirme *mutatis mutandis* que l'équation $x^\lambda + y^\lambda = z^\lambda$ n'a pas de solutions entières pour tous les nombres λ, premiers, impairs. Il y a lieu de démontrer ce théorème, soit en général suivant les idées de Fermat, soit en particulier conformément aux recherches de Kummer (*J. de Crelle*, t. XL, p. 130 ; *Abh. der Akad. d. Wiss.*, Berlin, 1857) pour tous les exposants λ, pour lesquels il a, en somme, une valeur.

Consulter Hilbert, *Theorie der algebraischen Zahlkörper* 1894-5 et *Encyklopädie*, 1900-1904.

La *Königliche Gesellschaft der Wissenchaften in Göttingen* décidera en toute liberté à qui le Prix doit être attribué. Elle refuse d'accepter tout manuscrit ayant pour objet de concourir à l'obtention du Prix ; elle ne prendra en considération que les mémoires mathématiques qui auront paru sous forme de monographie dans des journaux périodiques, ou qui sont en vente sous forme de volumes en librairie. La Société prie les auteurs de pareils mémoires de lui en adresser au moins cinq exemplaires imprimés.

Seront exclus du concours les travaux qui seraient publiés dans une langue qui ne serait pas comprise des savants spécialistes désignés pour le jugement. Les auteurs de pareils travaux pourront y substituer des traductions dont la fidélité soit certaine.

La Société décline toute responsabilité au sujet du non-examen de travaux dont elle n'aurait pas eu connaissance, ainsi que des erreurs qui pourraient résulter du fait que le véritable auteur du travail ou d'une partie du travail était inconnu de la Société.

Elle se réserve toute liberté de décision pour le cas où plusieurs personnes s'occuperaient de la solution de la question ou pour le cas où cette solution résulterait des travaux combinés de plusieurs savants, en particulier en ce qui concerne le partage du Prix, à son gré.

L'attribution du Prix par la Société aura lieu au plus tôt deux ans après la publication du mémoire à couronner. Cet intervalle de temps a pour but de permettre aux mathématiciens allemands et étrangers d'émettre leur opinion au sujet de l'exactitude de la solution publiée.

Dès que le Prix aura été attribué par la Société, le lauréat en sera informé par le secrétaire au nom de la Société, et le résultat sera publié partout où le Prix aura été annoncé pendant la dernière année écoulée. L'attribution du Prix par la Société est inattaquable.

Le paiement du Prix sera fait au lauréat, dans l'intervalle des trois mois qui suivront son attribution, par la caisse royale de l'Université de Göttingue, ou, aux risques et périls du destinataire, en un autre endroit qu'il aura désigné.

Le capital pourra être versé contre quittance, au gré de la Société, soit en argent comptant, soit par simple transmission des valeurs financières qui le constituent. Le paiement du Prix sera donc considéré comme effectué par la transmission de ces valeurs lors même que le total de leur valeur au cours du jour n'atteindrait pas 100 000 marks.

Au cas où le Prix n'aurait pas été délivré au 13 septembre

2007, aucune réclamation ultérieure ne serait plus admise.

Le concours pour le Prix Wolfskehl est ouvert à la date de ce jour aux conditions ci-dessus.

Göttingue, 27 juin 1908.

Die Königliche Gesellschaft der Wissenschaften.

§ XXII. — **Du dernier théorème de Fermat,**

par A. Wieferich, de Munster in Westphalien (*J. de Crelle*, t. CXXXV, p. 293, 1909). Couronné par la Société royale de Göttingue.

« M. Mirimanoff a formulé, comme critère de Kummer, la proposition suivante : si l'équation $x^p + y^p + z^p = 0$ est résoluble, x, y, z premiers entre eux et à p, les congruences

$$\varphi_i B_{\frac{p-i}{2}} \equiv 0 \pmod{p}$$

doivent être vérifiées par $i = 3, 5, \ldots (p-2)$, où B_i est le $i^{ème}$ nombre de Bernoulli et $\varphi_i = \sum_{j=1}^{p-1} (-1)^{j-1} t^j j^{i-1}$.

Dans le travail suivant, on va démontrer que vérifier ces congruences entraîne nécessairement la congruence

$$2^{p-1} \equiv 1 \pmod{p^2}. \text{ »}$$

La Société attribua à Wieferich 100 marks sur les intérêts de la Fondation Wolfskehl.

§ XXIII. — **Remarques sur le grand théorème de Fermat,**

par Albert Fleck (*Sitzungsbericht Berliner mathematischen Gesellschaft*, t. LXXII, p. 133, 1909 et t. LXXVIII, 1910).

« Après le grand progrès que Kummer a réalisé dans la recherche de la résolution de l'équation $x^p + y^p + z^p = 0$, la discussion du problème semble être entrée, pour un certain nombre d'années, dans une période d'attente. Seulement, Kronecker lui a consacré un mémoire en 1888.

« Le zèle d'obtenir dans ce domaine des progrès crût d'une manière gigantesque lorsque le docteur Wolfskehl fonda son Prix. Les flots de travaux qui virent le jour dans un temps très court dépassèrent, de beaucoup, par leur masse, la quantité des travaux précédents, sans pouvoir se mesurer en qualité, même de loin, avec un de ceux-ci.

« Dans ce qui va suivre, je veux exposer quelques remarques qui datent de l'année précédente et quelques-unes de 1886 ; certaines me sont venues plus tard à la suite de réflexions sur ce sujet.

« Je ne donnerai pas une résolution ; car je ne sais, à cause de l'éloignement du but, si je me suis rapproché de celui-ci. J'ai surtout voulu montrer que le problème peut être changé en un autre. »

L'auteur ne précise pas ce nouveau problème : ce n'est qu'à la fin de son mémoire qu'il écrit : le problème serait, comme il est facile de le voir, complètement résolu si l'on pouvait montrer qu'une des grandeurs A, B, C serait égale à 1, ou que deux des grandeurs J, K, L, J_1, K_1, L_1 seraient égales entre elles et aussi égales à 1.

§ XXIV. — Prétendues démonstrations du théorème de Fermat.

(*Archiv der Mathematik und Physik*, Leipzig und Berlin, t. XIV à XVII, 1909-10, sous le titre *Sprechsaal : Vermeintliche Beweise der Fermatschen Satzes*).

La floraison signalée par Albert Fleck s'est manifestée dans un grand nombre de publications et de manuscrits ; c'est précisément Albert Fleck, secondé par deux autres rapporteurs, Oscar Person et Ph. Mannenchen, qui en a rendu compte dans le périodique *Archiv*.

A la suite des tomes, on lit des suppléments, sous le titre : *Sitzungsberichte der Berliner Mathematischen Gesellschaft*.

Malheureusement, le rapporteur renvoie le lecteur à ces publications et manuscrits.

Dans les *Œuvres de Fermat,* t. IV, Compléments de Ch. Henry, on lit les noms de cinquante-et-un mathématiciens, anglais, belges, allemands, suisses, russes, qui ont publié des articles sur ce théorème. Pour douze d'entre eux, il renvoie le lecteur aux *Archiv.*

§ XXV. $x^n + y^n \neq z^n$, par ANDRÉ GÉRARDIN

(*Association française, Congrès pour l'Avancement des Sciences,* St-Étienne, 1897, p. 156 ; Lille, 1909, p. 143 ; Toulouse, 1910, pp. 43, 44, 55, et *C. R.,* t. CXV, p. 843, 1894).

Il fait l'historique de la question, cite cinquante auteurs, cent articles.

« Je crois que le théorème pourrait se démontrer en faisant voir que la différence de deux puissances $n^{\text{ièmes}}$ est toujours comprise entre deux puissances $n^{\text{ièmes}}$ consécutives.

« Enfin la somme de deux puissances $n^{\text{ièmes}}$ peut être égale à une puissance $n^{\text{ième}}$, augmentée ou diminuée de 1. Exemples : $9^3 + 10^3 = 12^3 + 1$, $6^3 + 8^3 = 9^3 - 1$. » (1)

§ XXVI. — **Sur le dernier théorème de Fermat et le critérium de M. Wieferich,**

par D. MIRIMANOFF (*Enseignement mathématique,* p. 455, 1909-10).

L'auteur rappelle la condition de Wieferich et la retrouve autrement. Ayant cité P. BACHMANN, *Niedere Zahlentheorie,*

(1) On retrouve ces exemples et on en obtient une infinité d'autres pour $n = 3$, en appliquant la relation d'Euler $x^3 + y^3 = z^3 - v^3$, où v serait égal à 1. En effet, Euler a exprimé les valeurs de x, y, z, v, solutions de cette égalité, sous forme entière, en fonction de quatre indéterminées f, g, h, k, et il a choisi, comme application, $h = 1$, $k = 0$. Or, si, dans les nouvelles expressions de x, y, z, v en fonction de f, g, on suppose $f = 3g$, on trouve $v = 1$, et l'égalité devient

$$(12^2g^4 - 6g)^3 + (6.12.g^3 - 1)^3 = (12^2g^4)^3 - 1,$$

où g est entier, positif ou négatif. Pour $g = \mp \frac{1}{2}$, on obtient les deux exemples cités.

Leipzig, il ajoute : « Le deuxième chapitre donne des indications intéressantes sur les méthodes appliquées à l'étude de ce grand problème, sur lequel s'est portée de nouveau l'attention des mathématiciens. »

§ XXVII. — Sur le théorème de Fermat,

par G. FROBENIUS, de Berlin (*Crelle*, 1909-10).

L'auteur reprend le résultat obtenu par Wieferich et Mirimanoff et y arrive, à son tour, simplement (1).

§ XXVIII. — Sur le dernier théorème de Fermat,

par D. MIRIMANOFF. Présentée par M. Appell (*C. R.*, Paris, 1910).

« Wieferich a prouvé (*Crelle*, t. CXXXVI) que si

$$x^p + y^p + z^p = 0$$

est vérifiée par des entiers premiers à p, le quotient de Fermat $q(2) = \dfrac{2^{p-1} - 1}{p}$ est divisible par p. Je ferai voir qu'il en est de même pour $q(3)$. »

§ XXIX. — Sur le dernier théorème de Fermat,

par D. MIRIMANOFF, à Genève (*Journal de Crelle*, t. CXXXIX, 1911).

« Est-il possible de généraliser le théorème de Wieferich ? Avant de chercher une réponse à cette question, il importait de simplifier la démonstration du géomètre allemand. Ce premier pas a été fait par M. G. Frobenius dans une note des *Sitzungsb. der Kgl. preuss Akad. d. Wiss. Berlin* du 2 décembre 1909, reproduite ici t. CXXXVII, et par l'auteur

(1) Si on applique à $p = 59, 67$, la condition nécessaire de Wieferich, on trouve

$$8280102733459 \times 3481 + 364,\quad 16437285875437337 \times 4489 + 670.$$

de ce travail dans *l'Enseignement mathématique* de novembre 1909. Il restait à généraliser les principes de ces démonstrations.

« Dans les *Comptes rendus* de Paris, janvier 1910, j'ai montré qu'à tout entier m, premier, on peut faire correspondre un polynome, qui, sous certaines conditions, se réduit à $mq(m)$. Pour $m = 2,3$, on retrouve les conditions connues ; mais, si $m > 3$, les critères deviennent moins simples. »

CHAPITRE VI

DE MIRIMANOFF A 1931

---

§ I. — **Le dernier théorème de Fermat démontré,**

par L. Gouy, Gauthier-Villars (1912).

L'auteur utilise la différence $(x+y)^n - x^n - y^n$, et la propriété de deux fractions irréductibles, de somme unité, d'avoir le même dénominateur.

§ II. — **Démonstration du théorème de Fermat,**

par E. Fabry, professeur à l'Université de Montpellier (*C. R.,* 1913).

L'auteur part d'un théorème de Kummer sur les nombres idéaux (*Crelle,* t. XXXV) et démontre que l'équation

$$x^\lambda + y^\lambda + z^\lambda = 0$$

est impossible : 1° si x, y ou z n'est pas divisible par λ ; 2° si l'un d'eux est divisible par λ sans l'être par λ^2.

§ III. — **Mémoires de M. H. S. Vandiver,** de Philadelphie.

De 1914 à 1929, l'auteur a publié, principalement dans les *Annals of Mathematics,* Washington, de nombreux et intéressants mémoires sur le théorème et sur le quotient de Fermat. Il y reprend les résultats obtenus par Sophie Germain, Kummer, Wieferich, Furtwängler, Mirimanoff, Sylvester ; il les étend ou les obtient d'une manière un peu différente.

On y trouve ces résultats :

$$x^p - x, y^p - y, z^p - z, x + y + z$$

divisibles par p^3, en supposant

$$x^p + y^p + z^p = 0\ ;\ (x+y)^p \equiv x + y \pmod{p^3},$$

en supposant xyz non divisible par p ; z divisible par $2p^3$, en supposant z divisible par p.

§ IV. — Sur la résolution de $x^n + y^n = z^n$,

par Joseph Joffroy (*Nouvelles Annales de Mathématiques*, t. XI, 1910.)

En généralisant la formule de Fermat $a^p - a = mp$, l'auteur prouve que, si l'équation admettait des solutions, les valeurs des inconnues seraient très grandes, quel que fût n.

§ V. $x^2 + y^2 = z^2$, $x^4 + y^4 = z^2$, $x^4 + y^4 = z^4$, $x^3 + y^3 = z^3$,

par Eugène Cahen, *Théorie des Nombres*, t. II, 1925.

Arrivé à l'équation du troisième degré, l'auteur applique le calcul des formes. Il démontre que l'équation du troisième degré n'est pas résoluble en nombres de la forme $a + bj$, et $x^4 + y^4 = z^2$ en nombres de la forme $a + bi$.

§ VI. — Sur le dernier théorème de Fermat,

par Léon Pomey (*C. R.*, 1923 et *Journal de Liouville*, t. IV, 9e série, 1925).

« Nous donnerons diverses conditions nécessaires sans lesquelles l'équation de Fermat est effectivement impossible. Nous les exposerons d'une manière aussi simple et concise que possible, sans d'ailleurs être obligé d'avoir recours aux méthodes et aux critères de Kummer.

« Elles ont été résumées dans une Note présentée à l'Académie des Sciences le 3 décembre 1923. »

Ayant, en particulier, établi trois théorèmes IV ter, V ter,

III bis, « ils paraissent être, écrit-il, en ce qui concerne le premier cas, les plus curieux de ceux que nous avons trouvés. Les théorèmes V bis et V ter ne sont pas évidemment sans faire penser aux conditions nécessaires bien connues de MM. Wieferich et Frobenius $2^{n-1}-1\equiv 0$ (mod. n^2) et de Mirimanoff $3^{n-1}-1\equiv 0$ (mod. n^2), obtenues, il est vrai, par ces géomètres à l'aide des critères de Kummer. »

L'auteur établit l'impossibilité de l'équation pour $n=59$, dans le premier cas. Il l'établit aussi pour $n=3, 5, 11, 17, 23, 29$, en s'aidant de tables dues à Jacobi.

Il applique à des valeurs de n, allant jusqu'à 5003249, le théorème de Sophie Germain, « qui a pu démontrer d'un trait de plume le théorème de Fermat dans le premier cas, pour $n < 100$ » et les critères de Legendre. Il est ainsi amené à chercher, même au delà de 5000000, les nombres premiers n tels que $2n+1$ soit. aussi, premier. Il traite de même le second cas.

§ VII. — Le dernier théorème de Fermat. État de la question,

par L. J. Mordell, professeur au Collège technique de Manchester, 1929.

L'auteur expose les démonstrations connues pour $n=2, 3, 5, 7$. Chemin faisant, il fait remarquer que Leibnitz a donné en 1678 une démonstration pour $n=4$, et que, sept cents ans avant Fermat, des mathématiciens indiens avaient donné les formules actuellement usitées pour $n=2$, ainsi qu'une démonstration inexacte de l'impossibilité pour $n=3$.

Viennent ensuite la décomposition des nombres algébriques, la théorie des nombres idéaux et leur application au théorème de Fermat ; à signaler la résolution de $x^2+y^2=z^n$.

Il rapporte que, d'après Dirichlet, Kummer avait pensé, comme Lamé et Cauchy, que les entiers algébriques en question ne pouvaient être décomposés en facteurs que d'une seule manière.

Au sujet des conditions $q^{p-1} \equiv 1 \pmod{p^2}$, il constate que q peut prendre la valeur 5, d'après VANDIVER (*Crelle*, t. CXLIV, 1915) et les valeurs 7, 13, 19, si $p = 5 + 6m$, d'après FROBENIUS (*Sitzungsberichte Ak. Wiss. Berlin*, 1914).

« En 1913, Meissner montra que $p = 1093$ est le seul nombre premier < 2000, pour lequel la congruence

$$2^{p-1} - 1 \equiv 0 \pmod{p^2}$$

est satisfaite. En d'autres termes, l'équation $x^p + y^p = z^p$, où p est premier, avec $2 < p < 2000$, ne peut être satisfaite par des valeurs premières à p, excepté peut-être quand $p = 1093$. »

L'auteur cite HILBERT qui, dans son Rapport sur *die Theorie der algebraischen Zahlkörper*, donne la version moderne de la théorie des Nombres idéaux.

Il cite aussi VANDIVER à propos du Mémoire de 1857, « contenant, avec quelques résultats complémentaires, quelques erreurs. »

Passant aux autres méthodes « d'attaque » du problème, il arrive à Libri et à Sophie Germain.

De LIBRI, il signale cet énoncé sans démonstration (*Crelle*, t. IX, 1832) : *Il n'existe pas un nombre infini de nombres premiers q, tels que, si $x^p + y^p + z^p$ est divisible par q, x, y ou z est nécessairement divisible par q.* « Cette proposition a été démontrée par M. A. PELLET, professeur à l'Université de Clermont-Ferrand (*Bulletin de la Société Mathématique*, t. XV, 1886-87, Paris) et par DICKSON et HURWITZ indépendamment en 1909 (*Crelle*, t. CXXXV, CXXXVI). »

Elle l'a été aussi par T. PÉPIN, pour $p = 3$ (*Comptes rendus*, t. XC, 1880).

De Sophie Germain, il explique le théorème, qu'il rattache aux découvertes de Legendre. Enfin, de Wendt, il dit : « le théorème de Sophie Germain fut présenté par WENDT sous une forme légèrement différente (*Crelle*, t. CXIII, p. 335, 1894). »

§ VIII. — Sur le théorème de Fermat,

par L. Massoutié (C. R., 5 octobre 1931. Présenté par M. d'Ocagne).

L'auteur démontre que, si p, premier, est de la forme $6n - 1$, une des indéterminées de $x^p + y^p + z^p = 0$ est nécessairement divisible par 3.

§ IX. — Nouvelles remarques,

par Léon Pomey (C. R., 12 octobre 1931. Présenté par M. d'Ocagne).

« Je suis depuis fort longtemps en possession du résultat communiqué par M. L. Massoutié. J'avais retardé la publication de ma démonstration, très différente de la sienne, pour achever les recherches entreprises en vue d'une généralisation encore inédite. »

L'auteur rappelle qu'il emploie les mêmes notations que dans sa seconde thèse, Journal de Liouville. J. M., 1925.

DEUXIÈME PARTIE

CHAPITRE VII

DE FERMAT A LEGENDRE

§ I. L'aire du triangle rectangle,

par FERMAT et LEGENDRE.

On a $(a^2+b^2)^2=(a^2-b^2)^2+(2ab)^2$; les nombres entre parenthèses représentent les côtés; aire $A=ab(a^2-b^2)$, a, b premiers relatifs.

Pour que A soit un carré, il faut que ses trois facteurs le soient; d'où $a=m^2$, $b=n^2$, et m^4-n^4 doit être un carré, ce qui entraîne $m^2+n^2=p^2$, $m^2-n^2=q^2$, et, par suite, $n^2+q^2=m^2$, $2n^2+q^2=p^2$.

p, diviseur de q^2+2n^2, est de forme f^2+2g^2. On posera donc $q+n\sqrt{-2}=(f+g\sqrt{-2})^2$, d'où q et n, et par suite $f^4+4g^4=m^2$.

Cette dernière équation représente un triangle rectangle, d'aire $A'=f^4g^4\neq 0$.

Je dis que $A'<A$. En effet,

$$A=4f^2g^2(f^2-2g^2)^2(f^2+2g^2)^2(f^4+4g^4).$$

Or, $f^2-2g^2\geqslant 1$, $(f^2+2g^2)^2>8f^2g^2$, $f^4+4g^4>4f^2g^2$.

Donc $$A'<\sqrt[3]{\frac{A}{128}}.$$

§ II. Traité des triangles rectangles en nombres,

par FRÉNICLE.

Ce traité, dont le fac-similé de la première page est reproduit ci-contre, est un petit livre de 116 pages, in-12, où l'auteur arrive, page 100, aux propositions XXXIX, XL :

Il n'y a aucun triangle rectangle en nombres, dont l'aire soit un nombre quarré.

Il n'y a aucun triangle rectangle en nombres, dont l'aire soit un double quarré.

Démonstrations par la descente infinie.

Conséquences de la proposition 39.

2ème conséquence. Il n'y a point de triangle rectangle auquel tant l'hypoténuse que le coté pair soit un nombre quarré ; parce que de ce triangle il en proviendrait un autre, dont le coté impair serait quarré et le pair un double quarré (proposition déjà établie), et, par conséquent, son aire serait un quarré.

4ème conséquence. Un quarré quarré impair ne peut être la somme d'un quarré quarré pair et d'un quarré impair : car les trois racines de ces trois carrés seraient un triangle rectangle, dont l'hypoténuse et le coté pair seraient quarrés, ce qui est contre la deuxième conséquence ; et, par la deuxième conséquence encore, un quarré impair ne peut être la différence de deux quarrés quarrés.

Conséquence de la proposition 40.

Première. Il n'y aucun triangle rectangle qui ait un quarré pour chacun de ses moindres cotés ; car l'aire serait un double carré.

Deuxième. Un quarré ne peut être la somme de deux quarrés quarrés ; parce que les racines de ces trois quarrés seraient les trois cotés d'un triangle, auquel chacun des deux moindres cotés seraient un quarré, contre la première conséquence.

TRAITÉ DES TRIANGLES RECTANGLES EN NOMBRES,

DANS LEQUEL PLUSIEURS belles proprietés de ces Triangles sont démontrées par de nouveaux principes.

Par Monsieur FRENICLE de l'Academie Royale des Sciences.

A PARIS,
Chez ESTIENNE MICHALLET, ruë Saint Jacques, à l'Image S. Paul proche la Fontaine S. Severin.

M. DC. LXXVI.

Avec Permission.

Troisième. Il n'y a aucun triangle rectangle primitif (dont les cotés n'ont d'autre commune mesure que l'unité) qui ait un quarré pour son hypoténuse et un double quarré pour son coté pair; parce que l'hypoténuse serait la somme de deux quarrés quarrés: ainsi on aurait un quarré qui serait la somme de deux quarrés quarrés, contre la deuxième conséquence.

Quatrième. Un quarré quarré ne peut être la somme de deux quarrés dont l'un ait pour racine un double quarré; parce que les racines de ces trois quarrés seraient les trois cotés d'un triangle, qui aurait un nombre quarré pour son hypoténuse et un double quarré pour son coté pair, contre la troisième conséquence.

§ III. $a^4 + b^4 = c^2$, $x^4 \pm y^4 = z^4$, par Legendre, 1823.

Théorème. — *La somme de deux bicarrés ne peut être égale à un carré.*

Si $a^4 + b^4 = c^2$ était possible, il faudrait d'abord que $a^2 = p^2 - q^2$, $b^2 = 2pq$, $c = p^2 + q^2$. a et b étant premiers relatifs, p et q le seront, l'un pair, l'autre impair; si p était pair, $p^2 - q^2$ serait de forme $4h - 1$, qui ne convient pas à a^2. Donc, de $b^2 = 2pq$, on tire $p = m^2$, $q = 2n^2$; d'où $a^2 = m^4 - 4n^4$, ou $m^4 = a^2 + 4n^4$.

Le seul moyen de satisfaire à cette équation est de prendre $m^2 = f^2 + g^2$, $n^2 = fg$, $a = f^2 - g^2$. On en tire, f et g étant premiers relatifs, $f = \alpha^2$, $g = \beta^2$, et, par suite, $\alpha^4 + \beta^4 = m^2$.

Je dis que α, β sont plus petits que a, b. En effet, $a = \alpha^4 - \beta^4$, $b = 2\alpha\beta\sqrt{\alpha^4 + \beta^4}$; ce qui donne

$$\alpha^4 + \beta^4 < \sqrt{\frac{a^2}{2} + \frac{1}{2}\sqrt{a^4 + b^4}},$$

et, par conséquent, $\alpha^4 + \beta^4 < \sqrt[4]{a^4 + b^4}$.

Corollaire. — La même démonstration prouve que

$$m^4 - 4n^4$$

ne peut être égal à un carré, et prouve à fortiori que x^4+y^4 ne peut être égal à z^4 ou $(z^2)^2$.

§ IV. $x^3 \pm y^3 = z^3$,

par Euler, 1774.

Théorème. — *La somme ou la différence de deux cubes ne peut être égale à un cube.*

Nous supposons x, y impairs, z pair, dans $x^3 \pm y^3 = z^3$.

Posons $\qquad x = p + q, \qquad y = p - q,$

d'où $x^3 + y^3 = 2p(p^2 + 3q^2)$, p et q de parités différentes. De même, $x^3 - y^3 = 2q(3p^2 + q^2)$.

Il faut donc prouver que $2p(p^2 + 3q^2)$ ne peut être un cube.

Si $2p(p^2 + 3q^2)$ est un cube, il est pair; donc p doit être divisible par 4. $2p$ et $p^2 + 3q^2$ ne peuvent avoir d'autre facteur commun que 3, et cela exige que p soit divisible par 3.

Premier cas : *p non divisible par* 3. $2p$ et $p^2 + 3q^2$ doivent être deux cubes. On posera donc

$$p + q\sqrt{-3} = (t + u\sqrt{-3})^3,$$

ce qui donne $p^2 + 3q^2 = (t^2 + 3u^2)^3$, et, par là, $p = t(t^2 - 9u^2)$, $q = 3u(t^2 - u^2)$. Puisque q est impair, t doit être pair.

Il s'agit maintenant que $2p$ soit un cube;

$$2p = 2t(t + 3u)(t - 3u)\,;$$

t n'est pas divisible par 3. Les trois facteurs, étant premiers entre eux, deux à deux, doivent être des cubes.

Soit $t + 3u = f^3$, $t - 3u = g^3$, d'où $2t = f^3 + g^3$. Si $2t$ est un cube, nous aurons ainsi deux cubes f^3, g^3 dont la somme serait un cube et qui seraient évidemment beaucoup plus petits que x^3 et y^3.

Si donc il existait dans les grands nombres deux cubes tels que nous les demandons, on pourrait en assigner en de moindres nombres dont la somme serait un cube, et, ainsi de suite. Or, il est certain qu'il n'y en a pas de pareils dans les

petits nombres; donc, il n'y en a pas dans les plus grands.

SECOND CAS : *p divisible par* 3. Soit $p = 3r$, d'où

$$x^3 + y^3 = 18r(q^2 + 3r^2);$$

$q^2 + 3r^2$ n'est divisible ni par 2, ni par 3, et r est pair comme p. Donc $18r$ et $q^2 + 3r^2$, premiers entre eux, doivent être deux cubes. Le second étant transformé comme ci-dessus, on trouve $q = t(t^2 - 9u^2)$, $r = 3u(t^2 - u^2)$.

q étant impair, t doit être impair et u pair.

Les trois facteurs de $18r$, $2u$, $t - u$, $t + u$, étant premiers deux à deux, doivent être des cubes. Soit $t + u = f^3$, $t - u = g^3$; d'où $2u = f^3 - g^3$. Si $2u$ est un cube, $f^3 - g^3$ le serait. On aurait, par conséquent, deux cubes beaucoup plus petits que les premiers et dont la différence serait un cube h^3, d'où $f^3 = g^3 + h^3$, et la conclusion serait la même que précédemment.

§ V. $x^3 \pm y^3 = z^3$,
par LEGENDRE.

Première démonstration.

Legendre reproduit celle d'Euler, en la complétant.

Des trois nombres, deux sont impairs; on peut les placer dans le même membre.

Si l'on fait $x \pm y = 2p$, $x \pm y = 2q$, on aura

$$2p(p^2 + 3q^2) = z^3;$$

p, q. l'un pair, l'autre impair. Mais $2p(p^2 + 3q^2)$ devant être un cube, p doit être divisible par 4.

PREMIER CAS : *p n'est pas divisible par* 3. Ayant posé $p = m(m^2 - 9n^2)$, $q = 3n(m^2 - n^2)$; et, plus loin, $m + 3n = a^3$, $m - 3n = b^3$, $2m = c^3$, l'auteur obtient l'équation $a^3 + b^3 = c^3$, et, par la substitution des valeurs précédentes,

$$z = abc\frac{a^6 + a^3b^3 + b^6}{3};$$

par conséquent, on a $z > a^4b^4c$, et à fortiori $z > c$.

SECOND CAS : *p est divisible par* 3. Ayant posé $p = 3r$, puis

$q = f(f^2 - 9g^2)$, $r = 3g(f^2 - g^2)$; et, plus loin, $f + g = a^3$, $f - g = b^3$, $2g = c^3$, l'auteur obtient l'équation $a^3 - b^3 = c^3$, et, par la substitution des valeurs précédentes,

$$z = 3abc(a^6 - a^3b^3 + b^6);$$

par conséquent, on a $z > 3a^4b^4c$, et, à fortiori, $z > c$.

Seconde démonstration.

Nous supposerons qu'il existe trois nombres entiers, positifs ou négatifs, l'un d'eux étant pair, premiers deux à deux, satisfaisant à $x^3 + y^3 + z^3 = 0$.

Notre démonstration sera divisée en trois parties.

1re PARTIE : *x, y ou z doit être divisible par* 3. Sinon, la somme des trois cubes aurait la forme $9n \pm 1$ ou $9n \pm 3$, et ne pourrait pas se réduire à zéro.

2e PARTIE : Si *z est pair, z est divisible par* 3. Soit $z = -2^m u$, u impair; d'où l'équation $x^3 + y^3 = 2^{3m}u^3$.

Supposons que u ne soit pas divisible par 3. Les deux facteurs $x + y$, $x^2 - xy + y^2$ de $x^3 + y^3$, ne pouvant avoir que 3 pour diviseur commun, sont donc premiers entre eux, et, par suite, sont des cubes. Comme $x^2 - xy + y^2$ est impair, on posera $x + y = 2^{3m}\alpha^3$, $x^2 - xy + y^2 = \beta^3$; d'où $u = \alpha\beta$, α, β premiers entre eux.

Maintenant, si on écrit

$$x^2 - xy + y^2 = \left(\frac{x+y}{2}\right)^2 + 3\left(\frac{x-y}{2}\right)^2,$$

on voit que β a la forme $f^2 + 3g^2$. Faisant ensuite

$$(f + g\sqrt{-3})^3 = F + G\sqrt{-3},$$

ce qui donne $F = f(f^2 - 9g^2)$, $G = 3g(f^2 - g^2)$, on aura $\beta^2 = F^2 + 3G^2$, de sorte qu'on satisfera généralement à l'équation précédente en prenant $\frac{x+y}{2} = F$, $\frac{x-y}{2} = G$. On obtient ainsi

$$x = f^3 + 3f^2g - 9fg^2 - 3g^3, \qquad y = f^3 - 3f^2g - 9fg^2 + 3g^3.$$

Or, z étant supposé non divisible par 3, il faudra que ce soit x ou y, ce qui exige que f le soit; mais alors x et y le seraient.

On posera donc $z = -2^m 3^n u$, u étant premier à 6.

3e PARTIE : $x^3 + y^3 = 2^{3m}3^{3n}u^3$ *est impossible.* Supposons pour un moment qu'elle soit possible. $x + y$ et $(x+y)^2 - 3xy$ ont 3 pour diviseur unique ; d'où

$$x + y = 2^{3m}3^{3n-1}\alpha^3, \qquad x^2 - xy + y^2 = 3\beta^3, \qquad u = \alpha\beta.$$

La seconde s'écrit $\beta^3 = \left(\frac{x-y}{2}\right)^2 + 3\left(\frac{x+y}{6}\right)^2$. Donc β est encore de forme $p^2 + 3q^2$. Soit $\beta = f^2 + 3g^2$, $\beta^3 = F^2 + 3G^2$; d'où $\left(\frac{x-y}{2}\right)^2 + 3\left(\frac{x+y}{6}\right)^2 = F^2 + 3G^2$, à laquelle on satisfait généralement en prenant $\frac{x-y}{2} = F$, $\frac{x+y}{6} = G$.

Cette dernière donne, en faisant les substitutions,

$$2^{3m-1} \,.\, 3^{3n-3}\alpha^3 = g(f^2 - g^2).$$

$f^2 - g^2$ est impair, puisque $f^2 + 3g^2$ l'est ; donc g doit être divisible par 2^{3m-1}. Soit $g = 2^{3m-1}A$, $f + g = B$, $f - g = C$.

On aura $(3^{n-1}\alpha)^3 = ABC$.

Maintenant, A, B, C étant premiers entre eux, on fera $A = \lambda^3$, $B = \mu^3$, $C = \nu^3$, ce qui donnera $f + g = \mu^3$, $f - g = \nu^3$, $g = 2^{3m-1}\lambda^3$, $\lambda\mu\nu = 3^{n-1}\alpha$.

On tire de là l'équation $\mu^3 - \nu^3 = 2g = 2^{3m}\lambda^3$, semblable à la proposée, où il faut observer que λ, μ ou ν doit contenir le facteur 3^{n-1}. Or, (2e partie) $2^m\lambda$, déjà divisible par 2, l'est nécessairement par 3 ; d'où $\lambda = 3^{n-1}\theta$, et $\mu^3 - \nu^3 = (2^m 3^{n-1}\theta)^3$.

Continuant ces transformations autant de fois qu'il y a d'unités dans n, on parviendra à une dernière transformée $x'^3 + y'^3 = z'^3$, dans laquelle aucun des nombres x', y', z' ne serait divisible par 3. Cette équation est impossible (1re partie) ; donc la proposée est, aussi, impossible.

§ VI. — Mémoire sur le théorème de Fermat,

par LEGENDRE.

Soit $x^n + y^n + z^n = 0$, où x, y, z sont supposés entiers et premiers deux à deux.

1. $x+y+z$ ou p est divisible par n; en effet, x^n-x, y^n-y, z^n-z et leur somme le sont.

De

$$y^n+z^n=(y+z)(y^{n-1}-zy^{n-2}+\cdots+z^{n-1})=(y+z)\varphi(y,z),$$

on déduit que ces deux derniers facteurs ont n pour commun diviseur unique ou n'en ont aucun, suivant que x est ou n'est pas divisible par n. Le facteur $y+z$ le contient $n-1$ fois; φ, une seule fois.

φ est impair et positif. On sait que 4φ peut se mettre sous la forme $Y^2\pm nZ^2$, n étant premier, de forme $4k\mp1$. (*Théorie des Nombres*, n° 509.)

2. Si x est divisible par n, $n(y+z)$ et $\frac{1}{n}\varphi(y,z)$ sont premiers entre eux, et sont, comme leur produit, des puissances $n^{\text{ièmes}}$. C'est pourquoi on posera $y+z=\frac{1}{n}a^n$, a divisible par n ou une puissance de n, et $\varphi=n\alpha^n$, d'où $x=-a\alpha$, α premier à na.

On aura ainsi les neuf équations

$$\begin{aligned}
&y+z=\frac{1}{n}a^n, &\quad &\varphi(y,z)=n\alpha^n, &\quad &x=-a\alpha,\\
&z+x=b^n, & &\varphi(z,x)=\beta^n, & &y=-b\beta,\\
&x+y=c^n, & &\varphi(x,y)=\gamma^n, & &z=-c\gamma,
\end{aligned}$$

avec

$$2x=-\frac{a^n}{n}+b^n+c^n,\qquad 2y=\frac{a^n}{n}-b^n+c^n,$$

$$2z=\frac{a^n}{n}+b^n-c^n.$$

Nous remarquerons que tout diviseur premier θ de α, β ou γ doit être de forme $2kn+1$. Car θ divise un nombre p^n+q^n sans diviser $p+q$; soit $p=qt+\theta u$. Il faudra que θ divise t^n+1 sans diviser $t+1$; d'où il suit que θ est de forme $2kn+1$ (*Théorie des Nombres*, 158).

De plus, tout diviseur premier de α est de forme $2hn^2+1$. L'auteur l'établit.

Si x n'est pas divisible par n, on remplacera dans les neuf équations $\frac{a^n}{n}$ par a^n et nx^n par x^n ; de même dans les suivantes.

3. Si x est divisible par n, il le sera par n^2, et p le sera également.

En effet, d'après $2p = \frac{a^n}{n} + b^n + c^n$, comme $2p$ et $\frac{a^n}{n}$ sont divisibles par n, $b^n + c^n$ le sera. Comme, d'ailleurs, $b^n - b$, $c^n - c$ sont divisibles par n, leur somme l'est et, par suite, $b + c$ l'est également.

Soit $b + c = nA$. On en déduit

$$b^n + c^n = nc^{n-1} \cdot nA - \frac{n(n-1)}{2} c^{n-2} n^2 A^2 + \cdots + (nA)^n.$$

Donc $b^n + c^n$ est divisible par n^2 ; comme $\frac{a^n}{n}$ est divisible par n^2, p le sera ; x, étant égal à $p - \frac{a^n}{n}$, le sera également.

4. Nous allons maintenant démontrer que x, y ou z est divisible par n.

Soit $q = xy + yz + zx$, $r = xyz$, d'où

$$V^3 - pV^2 + qV - r = 0$$

et x, y, z ses racines. On a

$$S_1 = p, \qquad S_2 = p^2 - 2q, \qquad S_3 = p^3 + 3(r - pq),$$

et, en général,

$$S_m = p^m - mqp^{m-2} + mrp^{m-3} + \frac{m(m-3)}{2} q^2 p^{m-4} - \frac{m(m-4)}{2} 2qrp^{m-5} + \frac{m(m-5)}{2} r^2 p^{m-6}$$
$$- \frac{m(m-4)(m-5)}{2 \cdot 3} q^3 p^{m-6} + \frac{m(m-5)(m-6)}{2 \cdot 3} 3q^2 rp^{m-7}, \text{ etc.}$$

Soit $n = 3$, on a $S_3 = 0$, d'où

$$p^3 = 3(pq - r) = 3(x + y)(y + z)(z + x).$$

Donc p est divisible par 3 et $y+z$, par exemple, par 9. Alors x le sera par 3 et même par 9.

Soit $n=5$, on a $S_5=0$, d'où

$$p^5=5(pq-r)(p^2-q)$$
$$=5(x+y)(y+z)(z+x)\frac{p^2+x^2+y^2+z^2}{2}.$$

Si aucun de $x+y$, $y+z$, $z+x$ n'est divisible par 5, il faudra que $x^2+y^2+z^2$ le soit. Or, le carré de tout nombre non divisible par 5 est de forme $5m\pm1$; la somme de trois nombres pareils est de forme $5m\pm1$ ou $5m\pm3$. Donc x, y ou z est nécessairement divisible par 5 et même par 25.

Ces deux premiers cas peuvent être démontrés plus simplement.

Un cube, par exemple, non divisible par 3, est de forme $9m\pm1$. Or, trois des restes ±1 ne peuvent faire la somme zéro, ni la somme 9.

Pour $n=7$, ce moyen ne réussit pas, mais il réussit pour 11 et 17. En effet, la puissance onzième d'un nombre non divisible par 11 est de forme $121m\pm(1, 3, 9, 27, 40)$. Or, dans ces restes, il n'y en a pas deux qui se suivent immédiatement; donc, trois de ces nombres ne peuvent faire ni la somme zéro, ni 121. Donc x, y ou z est divisible par 11.

Le principe dont nous venons de faire usage se démontre ainsi :

Supposons $x^n+y^n+z^n=0$ et θ un nombre premier non diviseur de xyz; x et θ^a sont premiers entre eux; on peut donc supposer $y=fx+\theta^a y'$, $z=gx+\theta^a z'$, et, en faisant la substitution, on verra que $1+f^n+g^n$ est divisible par θ^a, ou qu'en supprimant les multiples de θ^a, on a $(-g)^n=f^n+1$; donc, parmi les restes des puissances $n^{\text{ièmes}}$ divisées par θ^a, il y en aura toujours un, provenant de $(\theta-g)^n$ ou de $(-g)^n$ qui sera plus grand d'une unité que le reste provenant de f^n.

Si cette condition n'est pas remplie dans la série des restes, on doit en conclure qu'il y a nécessairement un des nombres x, y, z divisible par θ.

Revenons à $x^7+y^7+z^7=0$. La considération de S_7 est elle-même insuffisante. Il faut recourir à d'autres moyens.

On pourra faire $y+z=a^7$, $\varphi(y, z)=\alpha^7$, $x=-a\alpha$. Mais $4\varphi=Y^2+7Z^2$, où $Y=2y^3-y^2z-yz^2+2z^3$, $Z=yz(y-z)$. On aura donc $4\alpha^7=Y^2+7Z^2$, ou $\alpha^7=\left(\frac{Y}{2}\right)^2+7\left(\frac{Z}{2}\right)^2$, car Y, Z sont toujours pairs.

Cette équation fait voir que α, diviseur de la formule t^2+7u^2, doit être de même forme, $\alpha=f^2+7g^2$; faisant ensuite $(f+g\sqrt{-7})^7=F+G\sqrt{-7}$, ce qui donne

$$F=f(f^6-3\,.\,7^2f^4g^2+5\,.\,7^3f^2g^4-7^4g^6),$$
$$G=7g(f^6-5\,.\,7f^4g^2+3\,.\,7^2f^2g^4-7^2g^6).$$

On aura l'équation

$$\left(\frac{1}{2}Y\right)^2+7\left(\frac{1}{2}Z\right)^2=F^2+7G^2,$$

à laquelle on satisfait généralement par les valeurs

$$y^3+z^3-\frac{1}{2}yz(y+z)=F,\qquad \frac{1}{2}yz(y-z)=G.$$

Mais, puisque G est divisible par 7, il faudra que $yz(y-z)$, et, par suite, $y-z$ le soient aussi. En partant de $\varphi(z, x)$, on verrait de même que $x-z$ devrait l'être, et, par suite $3z$, aussi, ce qui est contre l'hypothèse.

Donc, enfin, pour $n=7$, x, y ou z doit être divisible par 7 et même par 49.

Le même mode de démonstration pourrait s'appliquer à 11 et à 19, mais pas à 13.

C'est pourquoi nous allons exposer une autre démonstration fort simple et d'une généralité presque absolue.

5. Soit, en effet, $x^n+y^n+z^n=0$, x, y, z non divisibles par n. Faisons voir que les équations du (2) ne peuvent avoir lieu.

Pour cela, supposons, ce qui sera prouvé ultérieurement,

qu'il existe pour chaque valeur de n un nombre premier $\theta = 2kn + 1$, tel qu'on ne peut pas satisfaire à l'équation $r' = r + 1$, r, r' étant deux résidus des puissances $n^{\text{ièmes}}$ divisées par θ, et tel en même temps que n ne soit pas un de ces résidus. Voici les conséquences de l'hypothèse x, y, z non divisibles par n.

Il faut d'abord que x, y ou z soit divisible par θ ; car, dans le cas contraire, on serait conduit comme précédemment (le principe se démontre ainsi) à l'équation $r' = r + 1$, qui n'a pas lieu. Soit ce nombre, x. Alors $b^n + c^n - a^n$ sera aussi divisible par θ, de sorte qu'en omettant les multiples de θ on aura aussi $b^n + c^n - a^n = 0$. Je conclus de cette dernière équation que l'un des nombres a, b, c est divisible par θ, sans quoi on serait conduit de nouveau à l'équation $r' = r + 1$, qui n'a pas lieu.

Ce nombre ne peut être ni b, ni c ; car, si cela était, x aurait un diviseur commun avec y ou z, exprimés par $-b\beta$, $-c\gamma$. Donc, c'est a.

Cela posé, en omettant toujours les multiples de θ, on aura les équations conditionnelles $x = 0$, $a = 0$, $b^n + c^n = 0$, $z = b^n$, $y = c^n$, $z = -y$. Ensuite, les valeurs $x = 0$, $z = -y$, étant substituées dans $\varphi(y, z) = \alpha^n$, $\varphi(z, x) = \beta^n$, $\varphi(x, y) = c^n$, il en résulte $ny^{n-1} = \alpha^n$, $z^{n-1} = \beta^n$, $y^{n-1} = \gamma^n$. Donc $n\gamma^n = \alpha^n$.

Mais, puisqu'on a $\theta = 2kn + 1$, si on appelle r un résidu quelconque de x^n non divisible par θ, on sait par les propriétés de ces résidus (*Théorie des Nombres,* 336) que les $2k$ valeurs de r qui satisfont à l'équation $\mu^{2k} = 1$ sont représentées par la suite 1, μ, μ^2, ... μ^{2k-1}, μ étant tel que $\mu^k = -1$ et qu'aucune autre puissance de μ dont le degré serait inférieur à k ne peut donner le reste -1. Il en résulte donc qu'on pourra faire $\alpha^n = \mu^i$, $\gamma^n = \mu^e$, et alors l'équation $n\gamma^n = \alpha^n$ donnerait $n = \mu^{i-e}$; donc n serait un résidu de puissance $n^{\text{ième}}$, ce qui est contre la supposition.

Tout se réduit par conséquent à prouver qu'il existe pour chaque valeur de n un nombre premier θ satisfaisant aux deux conditions mentionnées.

6. Voici un tableau à cet effet pour toutes les valeurs de n, moindres que 100.

n	θ	r	n	θ	r
3	7 = 2 . 3 + 1	± 1	47	659 = 14 . 47 + 1	± (1, 12, 55, 144, 249, 270, 307)
5	11 = 2 . 5 + 1	± 1			
7	29 = 4 . 7 + 1	± (1, 12)	53	107 = 2 . 53 + 1	± 1
11	23 = 2 . 11 + 1	± 1	59	827 = 14 . 59 + 1	± (1, 20, 124, 270, 337, 389, 400)
13	53 = 4 . 13 + 1	± (1, 23)			
17	137 = 8 . 17 + 1	± (1, 10, 37, 41)	61	977 = 16 . 61 + 1	± (1, 52, 80, 227, 252, 357, 403, 439)
19	191 = 10 . 19 + 1	± (1, 7, 39, 49, 82)			
23	47 = 2 . 23 + 1	± 1	67	269 = 4 . 67 + 1	± (1, 82)
29	59 = 2 . 29 + 1	± 1	71	569 = 8 . 71 + 1	± (1, 76, 86, 277)
31	311 = 10 . 31 + 1	± (1, 6, 36, 52, 95)	73	293 = 4 . 73 + 1	± (1, 136)
			79	317 = 4 . 79 + 1	± (1, 114)
37	149 = 4 . 37 + 1	± (1, 44)	83	167 = 2 . 83 + 1	± 1
41	83 = 2 . 41 + 1	± 1	89	179 = 2 . 89 + 1	± 1
43	173 = 4 . 43 + 1	± (1, 180)	97	389 = 4 . 97 + 1	± (1, 155)

On voit sur ce tableau que l'équation $r' - r = 1$ n'est satisfaite dans aucun cas. On voit de même que l'exposant n n'est pas compris parmi les valeurs de r. Ainsi, la proposition est démontrée pour les nombres < 100.

On peut remarquer que la valeur de k est un terme de la série 1, 2, 4, 5, 7, 8, où ne figure ni 3, ni 6. Cette suite s'étendrait plus loin si le tableau était prolongé, mais on n'y trouverait pas un multiple de 3. (L'auteur le prouve.)

Si l'on remarque que la valeur $\theta = 2n + 1$ s'applique à neuf des vingt-quatre cas considérés, on pourra présumer que, toutes les fois que $2n + 1$ est premier, il satisfera aux deux conditions prescrites.

L'auteur en dit autant pour $\theta = 4n + 1$, supposé premier, pour $8n + 1$, $16n + 1$, $10n + 1$, $14n + 1$, et il le prouve. « Ainsi, la proposition, démontrée par la table pour tous les nombres premiers n plus petits que 100, s'étend généralement à tous les nombres premiers n tels que, dans les six formules $2n + 1$, $4n + 1$, $8n + 1$, $10n + 1$, $14n + 1$, $16n + 1$, il y ait au moins un nombre premier ; ce qui permet d'étendre immé-

diatement la table jusqu'à $n = 197$, qui dépend du nombre premier $\theta = 38n + 1 = 7\,487$. »

7. « Dans le cas de $n = 5$, ces six formules donnent les nombres premiers 11, 41, 71, qui remplissent les deux conditions. La formule $10k + 1$ donne encore le nombre 101, qui satisfait aux deux conditions.

« Mais de 101 jusqu'à 1 000, on ne trouve aucun nombre $10k + 1$.

« Nous ne connaissons donc que quatre nombres qui divisent nécessairement x, y ou z dans $x^5 + y^5 + z^5 = 0$.

θ	RÉSIDUS CINQUIÈMES
11	± 1
41	$\pm(1, 3, 9, 14)$
71	$\pm(1, 20, 23, 26, 30, 32, 34)$
101	$\pm(1, 6, 10, 14, 17, 32, 36, 39, 41, 44)$

où l'équation $r' = r + 1$ n'est pas satisfaite et 5 ne figure pas dans les résidus. Cette dernière circonstance permet de démontrer que 11, 71, 101 divisent x, déjà divisible par 5^2, et, de plus, que cette propriété n'appartient qu'au plus petit a des deux facteurs a, α, dont x est composé. » Suit la démonstration.

« Il résulte de cette démonstration qu'on doit faire

$$a = 5^2 \,.\, 11 \,.\, 71 \,.\, 101 \,.\, a',$$

et, par suite, $y + z = \frac{1}{5}(5^2 \,.\, 11 \,.\, 71 \,.\, 101 \,.\, a')^5$; d'où l'on voit que y ou z serait composé de 31 chiffres au moins. »

L'auteur traite de même les cas de $n = 7, 11, 13, 17$. Dans le dernier, y ou z aurait au moins 78 chiffres.

« Ces exemples suffisent pour donner une idée de la grandeur des nombres qui satisferaient à l'équation de Fermat s'il y avait des cas de possibilité, ce qui est déjà fort peu probable. Procédons maintenant à la démonstration de l'impossibilité de l'équation pour $n = 5$. »

8. $$x^5 + y^5 + z^5 = 0,$$

par LEGENDRE.

Soit x divisible par 5; $y^5 + z^5 = -x^5$ se partage en deux équations :

$$y + z = 5^4 t^5, \qquad y^4 - y^3 z + y^2 z^2 - y z^3 + z^4 = 5 r^5$$

avec $x = -5tr$, r impair et premier à $5t$.

PREMIER CAS : x *pair*. t est pair. La seconde équation s'écrit

$$5\left(\frac{y^2 + z^2}{2}\right)^2 - \left(\frac{y^2 + 2yz + z^2}{2}\right)^2 = 5r^5,$$

ou

$$\left(\frac{y^2 + z^2}{2}\right)^2 - 5\left(\frac{5^7 t^{10}}{2}\right)^2 = r^5.$$

Comme le premier membre, son diviseur r est de forme $p^2 - 5q^2$; soit $r = f^2 - 5g^2$; puis, faisant

$$(f + g\sqrt{5})^5 = F + G\sqrt{5},$$

d'où

$$F = f(f^4 + 50 f^2 g^2 + 125 g^4),$$
$$G = 5g(f^4 + 10 f^2 g^2 + 5 g^4),$$

on aura $r^5 = F^2 - 5G^2$, et, par suite,

$$\left(\frac{y^2 + z^2}{2}\right)^2 - 5\left(\frac{5^7 t^{10}}{2}\right)^2 = F^2 - 5G^2.$$

Pour avoir une solution générale de cette équation, il faut prendre deux nombres m, n tels qu'on ait

$$(9 \pm 4\sqrt{5})^k = m + n\sqrt{5},$$

k étant un entier quelconque, ils satisferont en général à $m^2 - 5n^2 = 1$, et on pourra supposer

$$\frac{y^2 + z^2}{2} + \frac{5^7 t^{10}}{2}\sqrt{5} = (F + G\sqrt{5})(m + n\sqrt{5}),$$

ce qui donnera

$$\frac{1}{2}(y^2 + z^2) = mF + 5nG, \qquad \frac{1}{2} 5^7 t^{10} = mG + nF.$$

On peut réduire k aux restes, 0, ± 1, ± 2, de sa division par 5; il leur correspond les valeurs $m=1$, 9, 161, $n=0$, ± 4, ± 72. Mais on voit sur la dernière équation que nF doit être divisible par 5, et, comme f ne l'est pas, F ne l'est pas; donc, c'est n qui doit l'être; d'où $n=0$, $m=1$; ce qui donne une solution unique $\frac{1}{2}5^6t^{10}=g(f^4+10f^2g^2+5g^4)$.

Les deux facteurs du second membre sont premiers entre eux et g est pair. L'équation précédente donne donc lieu à deux autres

$$g=5^6 2^9 u^{10}, \qquad f^4+10f^2g^2+5g^4=r'^{10} \qquad \text{avec} \qquad t=2ur'.$$

Dans la seconde, le premier membre s'écrit

$$(f^2+5g^2)^2-5(2g^2)^2;$$

on peut donc poser $r'^2=f'^2-5g'^2$; ce qui donne

$$r'^{10}=\mathrm{F}'^2-5\mathrm{G}'^2,$$

F′, G′ étant des fonctions semblables à F, G.

On aura ainsi l'équation $(f^2+5g^2)^2-5(2g^2)^2=\mathrm{F}'^2-5\mathrm{G}'^2$, dans laquelle $2g^2=5^{12}2^{19}u^{20}$, et on trouvera, comme ci-dessus, que la seule solution est $5^{11}2^{19}u^{20}=g'(f'^4+10f'^2g'^2+5g'^4)$.

Faisant encore $u=u'r''$. r'' étant premier à $10u'$, on décomposera le second membre et on aura $g'=5^{11}2^{19}u'^{20}$, $f'^4+10f'^2g'^2+5g'^4=(r'')^{20}$.

Nous retombons ainsi sur des équations de même forme et dont la série peut se continuer indéfiniment. Or, ayant fait successivement $x=-5tr$, $t=2ur'$, $u=u'r''$, $u'=u''r'''$, etc., il s'ensuit que $t=2ur'=2u'r'r''=2u''r'r''r'''$, etc., de sorte que le nombre des facteurs r augmente continuellement dans l'expression de t.

Chacun de ces facteurs, déterminé par une équation de forme $r^{10m}=f^4+10f^2g^2+5g^4$, où f et g sont des nombres toujours croissants puisqu'on a $g'=\frac{1}{5}(2g^2)^2$, $f'^2>5g'^2$, est certainement plus grand que 1 et ne peut, comme nombre

entier, être moindre que 2. Donc, en supposant même que la suite $u, u', u'', \ldots$ eût pour limite 1, la valeur de t, composée d'un nombre indéfini de facteurs $2, r', r'', r''', \ldots$ surpassera bientôt toute quantité donnée, ce qui ne peut s'accorder avec la supposition faite que les valeurs primitives de x, y, z sont données en nombres finis.

Donc, l'équation proposée est impossible dans le premier cas.

Second cas : *x impair*. — La seconde équation peut s'écrire

$$\left(\frac{1}{2}yz\right)^2 - 5\left(\frac{y^2 - \frac{1}{2}yz + z^2}{5}\right)^2 = -r^5.$$

Faisant comme ci-dessus $(f+g\sqrt{5})^5 = F + G\sqrt{5}$, nous aurons $-r^5 = F^2 - 5G^2$ et l'équation à résoudre

$$\left(\frac{1}{2}yz\right)^2 - 5\left(\frac{y^2 - \frac{1}{2}yz + z^2}{5}\right)^2 = F^2 - 5G^2.$$

Supposant de nouveau $(9 \pm 4\sqrt{5})^k = m + n\sqrt{5}$, nous trouverons

$$\frac{1}{2}yz = mF + 5nG, \qquad \frac{1}{5}\left(y^2 - \frac{1}{2}yz + z^2\right) = mG + nF\,;$$

on tirera de ces équations

$$\frac{1}{5}(y+z)^2 = (m+n)F + (m+5n)G,$$

ou

$$5^7t^{10} = (m+n)F + (m+5n)G.$$

Puisque G est toujours divisible par 5 et que F ne l'est pas, il faut que $m+n$ soit divisible par 5. Or, d'après les cinq valeurs de m, n rapportées ci-dessus, cette condition exige que $m = 9$, $n = -4$, ce qui donnera $5^7t^{10} = 5F - 11G$, c'est-à-dire

$$5^6t^{10} = f^4(f - 11g) + 10f^2g^2(5f - 11g) + 5g^4(25f - 11g).$$

Cette équation montre que $f - g$ doit être divisible par 5.

Soit donc $f = g + h$, où h est divisible par 5, d'où

$$F + G\sqrt{5} = [h + g(1 + \sqrt{5})]^5.$$

On tire de là F, G, et 5F — 11G, ce qui donnera

$$5^6 t^{10} = h(h^4 - 6h^3 g + 16h^2 g^2 - 16hg^3 + 16g^4).$$

g n'est pas divisible par 5, h doit être impair ; on décomposera donc le second membre en deux équations

$$h = 5^6 u^{10}, \qquad h^4 - 6h^3 g + 16h^2 g^2 - 16hg^3 + 16g^4 = r'^{10}$$

avec $t = ur'$, r' premier à $5u$.

La seconde s'écrit $r'^{10} = (h^2 - 3gh + 6g^2)^2 - 5(gh - 2g^2)^2$; on posera donc $r'^2 = f'^2 - 5g'^2$; ce qui donnera

$$r'^{10} = F'^2 - 5G'^2,$$

et on satisfera à la précédente équation généralement en faisant

$$h^2 - 3gh + 6g^2 = mF' + 5nG', \qquad gh - 2g^2 = mG' + nF',$$

ce qui donne enfin

$$5^{12} u^{20} = (m + 3n)F' + (3m + 5n)G'.$$

G' étant divisible par 5, F' ne l'étant pas, il faut donc que $m + 3n$ le soit. Cette condition exige que $m = 161$, $n = -72$, ce qui donnera

$$5^{11} u^{20} = \frac{123}{5} G' - 11F',$$

c'est-à-dire

$$5^{11} u^{20} = f'^4(123g' - 11f') + 10f'^2 g'^2(123g' - 55f') \\ + 5g'^4(123g' - 275f').$$

Cette équation montre que $3g' - f'$ doit être divisible par 5.

Soit donc $f' = 3g' - h'$, où h' est divisible par 5 ; d'où

$$F' + G'\sqrt{5} = [-h' + g'(3 + \sqrt{5})]^5.$$

On tire de là F', G', $\frac{123}{5}G' - 11F'$, ce qui donnera

$$5^{11} u^{20} = h'(11h'^4 - 42h'^3 g' + 64h'^2 g'^2 - 48h' g'^3 + 16g'^4).$$

Le second membre se décompose ainsi :

$h' = 5^{11}u'^{20}, \quad 11h'^4 - 42h'^3g' + 64h'^2g'^2 - 48h'g'^3 + 16g'^4 = r''^{20}$

avec $u = u'r''$, r'' premier à $5u'$.

La seconde équation s'écrit

$$4r''^{20} = (8g'^2 - 12g'h' + 7h'^2)^2 - 5h'^4.$$

On posera donc $r''^4 = f''^2 - 5g''^2$, ce qui donnera

$$r''^{20} = F''^2 - 5G''^2.$$

Soit maintenant $4 = \mu^2 - 5\nu^2$, μ et ν impairs. On pourra supposer

$$8g'^2 - 12g'h' + 7h'^2 + h'^2\sqrt{5} = (F'' + G''\sqrt{5})(\mu + \nu\sqrt{5});$$

ce qui donne $h'^2 = \mu G'' + \nu F''$.

h' et G'' étant divisibles par 5 et F'' ne l'étant pas, il faut que ν le soit, et, comme on a en général

$$(\mu + \nu\sqrt{5}) = (3 + \sqrt{5})(m + n\sqrt{5}),$$

d'où l'on tire $\mu = 3m + 5n$, $\nu = m + 3n$. on ne pourra admettre que $m = 161$, $n = -72$, d'où résultent $\mu = 123$, $\nu = -55$; ce qui donne

$5^{22}u'^{20} = 123G'' - 55F''$, équation semblable à une équation déjà considérée. Il en résulte que les mêmes transformations peuvent être continuées à l'infini. ce qui supposerait infinies les valeurs primitives de x, y, z. »

Comme dans le premier cas, l'auteur justifie cette dernière assertion.

L'équation proposée est donc impossible dans le second cas.

§ VII. $x^n = y^n + z^n$,

par ABEL (1823).

THÉORÈME I. — *L'équation est impossible quand une ou plusieurs des quantités $x, y, z, x+y, y+z, z+x$ sont des nombres premiers.*

Théorème II. — *Si l'équation est satisfaite, x, y, z seront décomposables en deux facteurs premiers entre eux au, bv, cw, et l'un des cinq cas suivants aura lieu :*

$$2x = +a^n + b^n + c^n, \qquad 2y = a^n - b^n + c^n,$$
$$2x = +n^{n-1}a^n + b^n + c^n, \qquad 2y = n^{n-1}a^n - b^n + c^n,$$
$$2x = +a^n + n^{n-1}b^n + c^n, \qquad 2y = a^n - n^{n-1}b^n + c^n,$$
$$2x = n^{n-1}(+a^n + b^n + c^n), \qquad 2y = n^{n-1}(a^n - b^n + c^n),$$
$$2x = +a^n + n^{n-1}(b^n + c^n), \qquad 2y = a^n + n^{n-1}(-b^n + c^n),$$
$$2z = a^n + b^n - c^n;$$
$$2z = n^{n-1}a^n + b^n - c^n;$$
$$2z = a^n + n^{n-1}b^n - c^n;$$
$$2z = n^{n-1}(a^n + b^n - c^n);$$
$$2z = a^n + n^{n-1}(b^n - c^n).$$

Théorème III. — *Pour que l'équation soit possible, il faut que $2x$ ait une des formes* $a^n + b^n + c^n$, $a^n + b^n + n^{n-1}c^n$, $a^n + n^{n-1}(b^n + c^n)$.

Théorème IV. — *La quantité $2x$ ne peut être moindre que* $9^n + 5^n + 4^n$, *et la plus petite de $2x$, $2y$, $2z$ moindre que* $9^n - 5^n + 4^n$.

Si, par exemple, $n = 7$, la plus petite valeur de $2z$ est $9^7 - 5^7 + 4^7$, c'est-à-dire $4782969 - 78125 + 16384$, ou 4721228, les valeurs de $2x$, $2y$ seront $9^7 + 5^7 + 4^7$, $9^7 + 5^7 - 4^7$, c'est-à-dire 4877478, 4844710.

Mais ces nombres substitués dans l'équation ne la vérifient pas.

§ VIII. $x^5 + y^5 + z^5 = 0$,

par Lejeune-Dirichlet (1825).

D'abord quatre théorèmes préliminaires, dont celui-ci (4ᵉ) : Les nombres P, Q, devant être premiers relatifs, de parités différentes, Q devant être divisible par 5, je dis que pour égaler $P^2 - 5Q^2$ à une 5ᵉ puissance, de la manière la plus générale, il suffit de poser $P + Q\sqrt{5} = (\varphi + \psi\sqrt{5})^5$, les indéterminées φ, ψ étant premiers relatifs, de parités différentes, P non divisible par 5.

Théorème V. — *Les nombres m, n étant positifs, $n > 2$, A n'étant pas divisible ni par 2, ni par 5, ni par aucun nombre premier $10k+1$, je dis qu'il sera impossible de trouver deux nombres x, y, premiers relatifs, tels que $x^5 \pm y^5 = 2^m 5^n A z^5$.*

Soit $x \pm y = 2p$, $x \mp y = 2q$; l'équation se change, en posant $p = 2r$, en celle-ci :

$$r(q^4 + 2.5^2q^2r^2 + 5^3r^4) = 2^{m-1}5^{n-2}Az^5,$$

où r est divisible par 5.

Choisissons μ, ν positifs, tels que $m+\mu-1$, $n+\nu-2$ soient divisibles par 5, et B qui n'ait d'autres diviseurs premiers que ceux de A et tel que AB soit une 5ᵉ puissance. — Multiplions l'équation par $2^\mu 5^\nu B$; elle se change en

$$2^\mu 5^\nu Br(q^4 + \ldots) = 2^{m+\mu-1}.2^{n+\nu-2}ABz^5,$$

où le second membre est une 5ᵉ puissance.

L'auteur démontre que les deux facteurs du premier sont premiers relatifs; le trinome, en particulier, peut donc être égalé à une 5ᵉ puissance. Il s'écrit $(q^2+5^2r^2)^2 - 5(10r^2)^2$, de sorte que le premier théorème préliminaire lui est applicable, et on en déduit

$$q^2 + 5^2r^2 = t(t^4 + 25^2t^2s^2 + 5^3s^4),\ 10r^2 = 5s(t^4 + 10t^2s^2 + 5s^4).$$

Multipliant par $2^{2\mu-1}5^{2\nu-1}B^2$ la dernière équation, on obtient

$$2^{2\mu}.5^{2\nu}B^2r^2 = 2^{2\mu-1}5^{2\nu}B^2s(t^4 + \ldots).$$

Le premier membre est une 5ᵉ puissance, comme carré d'une 5ᵉ puissance; il en est donc de même du second, qu'on écrit simplement

$$2^g5^hCs(t^4 + \ldots). \qquad (\beta)$$

Le trinome $(t^2+5s^2)^2 - 5(2s^2)^2$, traité comme ci-dessus, donne lieu à des nombres s', t', analogues de s, t, et l'on a

$$5^2s'^5 < 2s^2.$$

Quelque loin qu'on prolonge les séries s, s', ..., t, t' ..., on ne rencontre jamais un terme égal à zéro. On doit donc conclure que (β) n'est pas une 5ᵉ puissance.

Le théorème V est donc établi.

L'auteur considère ensuite l'équation $x^5 \pm y^5 = z^5$.

Soit z divisible par 5.

Si z est pair, on pourra le remplacer par $2.5.z$, d'où $x^5 \pm y^5 = 2^5.5^5.z^5$, équation impossible d'après le théorème V.

Si z est impair, l'auteur, dans un second article, modifie le théorème IV : il remplace la formule

$$P + Q\sqrt{5} = (\varphi + \psi\sqrt{5})^5$$

par $P + Q\sqrt{5} = \frac{(\varphi + \psi\sqrt{5})^5}{16}$, et la démonstration est analogue.

CHAPITRE VIII

DE LEGENDRE A LAMÉ

---

§ I. $t^{14} = u^{14} + v^{14}$,

par Lejeune-Dirichlet (1832).

Le nombre pair sera u ou v. S'il y en a un divisible par 7, ce ne saurait être t, puisque 7 ne peut diviser la somme de deux carrés, premiers relatifs ; soit alors v.

L'équation s'écrit

$$(t^2 - u^2)[(t^2 - u^2)^6 + 7t^2u^2(t^4 - t^2u^2 + u^4)^2] = v^{14}.$$

t et u étant supposés premiers relatifs, $t^2 - u^2$ et tu le seront, et aussi $t^2 - u^2$ et $t^4 - t^2u^2 + u^4$, qui s'écrit

$$(t^2 - u^2)^2 + t^2u^2.$$

Pour abréger, posons $\varphi = t^2 - u^2$, $\psi = tu(t^4 - t^2u^2 + u^4)$; φ, ψ premiers relatifs, de parités différentes.

L'équation devient $\varphi[(\varphi^3)^2 + 7\psi^2] = v^{14}$.

Premier cas. *v non divisible par* 7.

φ n'est pas divisible par 7 et les deux facteurs du premier membre sont des 14^{ièmes} puissances. D'un autre côté, on conclut d'un théorème connu que la racine de la 14ième puissance impaire $(\varphi^3)^2 + 7\psi^2$ a la même forme $g^2 + 7h^2$ et l'on prouve facilement que les entiers g, h satisfont à l'équation

$$\varphi^3 + \psi\sqrt{-7} = (g + h\sqrt{-7})^{14},$$

où il faut égaler séparément les parties réelles et les coefficients de $\sqrt{-7}$.

Sans développer cette expression, il est évident que la

valeur qu'elle donne pour ψ est divisible par 7; par suite t ou u doit l'être, ce qui serait contraire à l'hypothèse faite.

Ce premier cas ne peut donc avoir lieu.

DEUXIÈME CAS. *v divisible par* 7; $v = 7w$, d'où

$$t^{14} - u^{14} = 7^{14}w^{14}.$$

Sans compliquer l'opération, nous pouvons traiter l'équation plus générale $t^{14} - u^{14} = 2^m . 7^{1+n}w^{14}$, $m, n \geqslant 0$, qui devient en posant $\varphi = 7X$, $7^2X[\psi^2 + 7(7^2X^3)^2] = 2^m . 7^{1+n}w^{14}$. Les deux facteurs du premier membre, dont le second est impair, sont premiers relatifs; ils sont donc des 14^{ièmes} puissances, au facteur près 2^m7^{1+n} pour 7^2X.

D'après ce qu'on a vu plus haut, la seconde condition exige que $\psi + 7(7^2X^3)\sqrt{-7} = (r + s\sqrt{-7})^{14}$, c'est-à-dire $7^2X^3 = \dfrac{(r + s\sqrt{-7})^{14} - (r - s\sqrt{-7})^{14}}{2\sqrt{-7}}$; r, s premiers relatifs, de parités différentes, r non divisible par 7.

Transformant le numérateur comme précédemment $t^{14} - u^{14}$, on a $7^6X^3 = 2 . 7^5 . rs[R + 7(4rs)^3][R - 7(4rs)^3]$,

où $$R = (r^2 + 7s^2)(r^4 - r^2s^2 + 7^2s^4).$$

Les trois facteurs, étant premiers relatifs, sont des puissances 14^{ièmes}, le premier, au facteur près $2^{3m} . 7^{3+3n}$; d'où $2 . 7^5rs = 2^{3m} . 7^{3+3n}v'^{14}$, $R + 7(4rs)^3 = t'^{14}$, $R - 7(4rs)^3 = u'^{14}$.

On en déduit $t'^{14} - u'^{14} = 2^{9m+4} . 7^{3n'+4}w'^{14}$, avec $w' = v'^3$. Cette équation est entièrement semblable à l'équation de départ, dont elle dérive; seulement, t', u', premiers relatifs, sont plus petits que t, u. On en conclut, à la manière ordinaire, que $t^{14} = u^{14} + v^{14}$ est impossible.

§ II. $x^{2\lambda} + y^{2\lambda} = z^{2\lambda}$,

par KUMMER (1837).

On sait que, dans $(z - y)\varphi(y, z) = x^n$, $z - y$ ou $n(z - y)$, suivant que x n'est pas ou est divisible par n, est une puissance $n^{ième}$.

C'est le cas ici de z^2-y^2, z^2-x^2, et, par suite, de $z-y$, $z+y$, $z-x$, $z+x$, qui deviennent des puissances $\lambda^{ièmes}$. Bornons-nous au cas où y est pair et contient le facteur 2^ν et où x n'est pas divisible par λ.

Une des expressions trouvées est $z-x=2^{2\lambda\nu-1}q^{2\lambda}$, où q divise y.

C'est aussi le cas de $z^{2\lambda}-x^{2\lambda}$, et, par suite, de $z^\lambda+x^\lambda$, $z^\lambda-x^\lambda$, qui deviennent $2C^{2\lambda}$, $2^{2\lambda-1}D^{2\lambda}$; ce qu'on écrit

$$z^\lambda - C^{2\lambda} = 2^{2\lambda\nu-2}D^{2\lambda}, \qquad C^{2\lambda} - x = 2^{2\lambda\nu}\,.\,D^{2\lambda}.$$

De ces formules résultent les suivantes : $z-C^2=2^{2\lambda\nu-2}r^{2\lambda}$. $C^2-x=2^{2\lambda\nu-2}s^{2\lambda}$, et, par suite, $z-x=2^{2\lambda\nu-2}(r^{2\lambda}+s^{2\lambda})$, d'où, finalement, $r^{2\lambda}+s^{2\lambda}=2q^{2\lambda}$, r, s diviseurs de D et, par suite, de y.

THÉORÈME. — *Si l'équation $x^{2\lambda}+y^{2\lambda}=z^{2\lambda}$ est résoluble, on peut trouver trois nombres, facteurs de y, r, s, q, qui satisfont à $r^{2\lambda}+s^{2\lambda}=2\,.\,q^{2\lambda}$.*

§ III. $x^7+y^7=z^7$,

par LAMÉ (1839).

L'équation s'écrit

$$x^7=(z-y)\left[(z-y)^6+7y(z-y)^5+\cdots+7y^6\right]=(z-y)X.$$

PREMIER CAS : *x, y, z non divisibles par* 7. — Les nombres X, $z-y$, Y, $z-x$, Z, $x+y$ sont tous premiers entre eux, d'où les décompositions

$$\begin{aligned} z-y&=\mu^7, & X&=m^7, & x&=m\mu,\\ z-x&=\nu^7, & Y&=n^7, & y&=n\nu,\\ x+y&=\rho^7, & Z&=p^7, & z&=p\rho; \end{aligned}$$

m, μ, ... sont tous premiers entre eux.

Ces équations donnent

$$x+y-z=\mu(m-\mu^6)=\nu(n-\nu^6)=\rho(\rho^6-p)=A\mu\nu\rho,$$

où A est un nombre entier, premier avec μ, ... m ... x, y, z.

On trouve

$$\rho^7 - \nu^7 - \mu^7 = 2A\mu\nu\rho, \qquad 2x = \mu^7 - \nu^7 + \rho^7,$$
$$2y = -\mu^7 + \nu^7 + \rho^7, \qquad 2z = \mu^7 + \nu^7 + \rho^7,$$

d'où $(\mu^7 - \nu^7 + \rho^7)^7 + (-\mu^7 + \nu^7 + \rho^7)^7 = (\mu^7 + \nu^7 + \rho^7)^7$.

Mais on a généralement

$$(c+b+a)^7 - (c-b+a)^7 - (c+b-a)^7 + (c-b-a)^7$$
$$= 7\,.\,8abc[3(a^4 + b^4 + c^4) + 10(a^2b^2 + b^2c^2 + c^2a^2)].$$

Si l'on pose $\mu^7 = a$, $\nu^7 = b$, $\rho^7 = c$, on en déduit

$$2^4A^7 = 7[3(a^4 + b^4 + c^4) + 10(a^2b^2 + b^2c^2 + c^2a^2)].$$

On va démontrer que A, déjà divisible par 7, est un carré. Résolue en a^2, cette dernière équation donne

$$3a^2 = -5(b^2 + c^2) + 2\sqrt{4b^4 + 5b^2c^2 + 4c^4 + \frac{12}{7}A^7},$$

qu'on écrit $3a^2 = -5\psi + 2\varphi$, en posant

$$b^2 + c^2 = \psi, \qquad \frac{12}{7}A^7 = \varphi^2 + 3b^2c^2 - 4\psi^2.$$

En désignant $\mu\nu\rho$ par P, on a

$$a = c - b - 2AP,$$

d'où
$$a^2 = \psi - 2cb - 4AP(c - b - AP)$$

et, en remarquant que

$$c - b - AP = a + AP = x, \qquad a^2 = \psi - 2cb - 4APx.$$

Égalons les deux valeurs de a^2; on obtient

$$\varphi = 4\psi - 3cb - 6APx,$$

d'où

$$A\left[\frac{A^6}{7} + Px(4\psi - 3cb - 3APx)\right] = (\psi - cb)^2.$$

Or, A est premier avec P et avec x; donc tout facteur premier, commun à A et à la quantité entre crochets, diviserait $4\psi - 3cb$ et $\psi - cb$, et par suite cb ou $\rho^7\nu^7$, ce qui n'est pas. Les deux facteurs de gauche étant premiers entre

eux, on en déduit la décomposition

$$A = B^2, \qquad \frac{A^6}{7} + Px(4\psi - 3cb - 3APx) = G^2,$$
$$b^2 - cb + c^2 = BG.$$

Donc A est un carré.

Si on pose $G - 2BPa = D$, la dernière des trois équations devient $a^2 + b^2 + c^2 - bc - ca + ab = BD$. A celle-ci joignons les relations suivantes, déjà considérées,

$$abc = P^7, \qquad c - a - b = 2B^2P,$$
$$3(a^4 + b^4 + c^4) + 10(a^2b^2 + b^2c^2 + c^2a^2) = \frac{16}{7}B^{14}.$$

Nous formons un système de quatre équations, entre lesquelles on élimine a, b, c. On obtient

$$7\left(\frac{B^6}{7}\right)^2 - D^2 = -P^8 - 5B^3P^2D + 7B^6P^4.$$

Or cette équation est impossible. En effet, on voit sur $x + y + z = AP$ que P est pair et A impair ; d'où B impair également. D'autre part, un des nombres a, b, c étant pair, BD et, par suite, D est impair. Il résulte de là que $\left(\frac{B^6}{7}\right)^2$ et D^2 étant de la forme $8n + 1$, le premier membre a la forme $8n + 6$ ou $4i + 2$, tandis que le second membre, divisible par P^2, a la forme $4i$.

Par conséquent, l'équation $x^7 + y^7 = z^7$ est impossible dans le premier cas.

Deuxième cas : *x, y ou z divisible par* 7. — Soit d'abord x divisible par 7. Par suite, $z - y$ l'est par 7^6 et X par 7. Les anciennes équations deviennent

$$z - y = 7^6\mu^7 = a, \qquad X = 7m^7, \qquad x = 7m\mu,$$
$$z - x = \nu^7 = b, \qquad Y = n^7, \qquad y = n\nu,$$
$$x + y = \rho^7 = c, \qquad Z = p^7, \qquad z = p\rho,$$
$$x + y - z = 7\mu(m - 7^5\mu^6) = \nu(n - \nu^6)$$
$$= \rho(\rho^6 - p) = 7A\mu\nu\rho = 7AP,$$
$$c - a - b = 2 . 7 . AP.$$

A est premier avec 7P, avec m, n, p, et avec x, y, z.
A est impair, P est pair, m, n, p sont impairs.
On a actuellement

$$7abc = (7\mu\nu\rho)^7, \qquad c - b - a = 2.7.\mathrm{AP},$$
$$-2^4\mathrm{A}^7 = 3(a^4 + b^4 + c^4) + 10(b^2c^2 + c^2a^2 + a^2b^2).$$

Si z, au lieu de x, est divisible par 7, c'est à la même dernière équation que l'on aboutit. On résoudra donc, comme dans le premier cas, l'équation en a^2 et on trouvera l'équation $\mathrm{A}[\mathrm{A}^6 + 7\mathrm{P}x(4\psi - 3bc - 3.7.\mathrm{AP}x)] = (\psi - bc)^2$, qu'on traitera de même. On parvient ainsi à une équation en B, P, D, comme précédemment. Pour simplifier, on est amené à poser

$$\mathrm{D} = \mathrm{D}_1 + \frac{5}{2}7^2\mathrm{P}^2\mathrm{B}^3,$$

d'où
$$\mathrm{B}^{12} - \mathrm{D}_1^2 = -7(7^3\mathrm{P}^4)^2 + 3\left(\frac{1}{2}7^2\mathrm{P}^2\mathrm{B}^3\right)^2.$$

« Cette dernière équation ne présente plus la même incompatibilité de forme que l'équation analogue du premier cas; aussi la démonstration de son impossibilité exige une recherche plus laborieuse.

D'abord, P étant pair et même de forme $4i$, je pose $\mathrm{P} = 2\mathrm{P}_0$ et j'obtiens

$$\mathrm{D}_1^2 = (\mathrm{B}^6 - 6.7^4\mathrm{P}_0^4)^2 + 7(2.7^3\mathrm{P}_0^4)^2.$$

Pour satisfaire à cette équation on pourrait s'appuyer sur des théorèmes concernant les formes quadratiques et leurs diviseurs; mais, sans rien emprunter à des théories étrangères, il suffit ici de résoudre directement l'équation indéterminée $t^2 = u^2 + 7v^2$, t, u impairs, v pair, premiers entre eux. »

Partant de $(t-u)(t+u) = 7v^2$, l'auteur décompose le premier membre et obtient

$$t = f^2 + 7g^2, \qquad \pm u = f^2 - 7g^2, \qquad v = 2fg,$$

comme solution de l'équation; c'est-à-dire, actuellement,

$$\mathrm{D}_1 = f^2 + 7g^2, \qquad \pm\mathrm{B}^6 \mp 6.7^4.\mathrm{P}_0^4 = f^2 - 7g^2, \qquad fg = 7^3\mathrm{P}_0^4,$$

où f n'est pas divisible par 7 et f, g sont premiers entre eux. De ceci, on déduit la décomposition $f = Q_1^4$, $g = 7^3P_1^4$, $P_0 = Q_1P_1$, où Q_1 et $7P_1$ sont premiers entre eux, Q_1 et P_1 de parités différentes.

L'équation en B, P_0 devient alors

$$(Q_1^4 + 3 \,.\, 7^4P_1^4)^2 = (B^3)^2 + 7(2^3 7^3 P_1^4)^2,$$

encore de forme $t^2 = u^2 + 7v^2$.

A la suite de plusieurs transformations successives, analogues à la précédente, l'auteur est amené à écrire d'abord l'équation $Q_1^4 = Q_2^8 - 3 \,.\, 7^4P_2^4Q_2^4 + 2^4 \,.\, 7^7P_2^8$ et plus loin l'équation $Q_5^4 = Q_6^8 - 3 \,.\, 7^4P_6^4Q_6^4 + 2^4 \,.\, 7^7P_6^8$, de même forme et composée de nombres beaucoup plus petits.

On en déduit l'impossibilité de ces équations, et par suite celle de $x^7 + y^7 = z^7$.

« Pour s'assurer de la grandeur relative des deux solutions, il suffira de remarquer que $P_2 = 2Q_3Q_4Q_5Q_6P_6$. Le nombre P_6, homologue de P_2, et étant nécessairement pair, ainsi que $P_5 = Q_6P_6$, ne peut être moindre que 2 ; $g_4 = 7^3P_5^4$ est donc $> 7^3 2^4$; $Q_3 = \sqrt{f_4^2 + 7g_4^2}$ surpasse donc $\sqrt{1 + 7^7 2^8}$, et, à plus forte raison, Q_3 surpasse $2^5 7^3$ ou 10976.

Ainsi, P_6 est au moins 22 000fois plus petit que P_2. »

§ IV. $x^7 + y^7 + z^7 = 0$,

par LEBESGUE (1840).

L'auteur part de l'équation

$$p^2 = q^4 - 2^{2a} \,.\, 3 \,.\, 7^4q^2r^2 + 2^{4a+4} \,.\, 7^7r^4,$$

où p, q, r sont impairs, premiers relatifs et $a > 1$.

THÉORÈME. — *Cette équation est impossible.*

Elle s'écrit

$$(p + q^2 - 2^{2a-1} \,.\, 3 \,.\, 7^4r^2)(p - q^2 + 2^{2a-1} \,.\, 3 \,.\, 7^4r^2) = 2^{4a-2}7^7r^4,$$

d'où, en posant $r = ts$,

$$p + q^2 - 2^{2a-1} \,.\, 3 \,.\, 7^4t^2s^2 = 2s^4,$$
$$p - q^2 + 2^{2a-1} \,.\, 3 \,.\, 7^4t^2s^2 = 2^{4a-3} \,.\, 7^7t^4,$$

d'où l'on tire

$$q^2 = s^4 + 2^{2a-1} \,.\, 3 \,.\, 7^4 s^2 t^2 - 2^{2a-4} \,.\, 7^7 t^4.$$

Traitant celle-ci comme la première, on finit par arriver à l'équation impossible, x, y, z impairs,

$$x^2 = y^4 - 2^2 \,.\, 3 \,.\, 7^4 y^2 z^2 - 2^8 7^7 z^4.$$

THÉORÈME. $x^7 + y^7 + z^7 = 0$ *est impossible.*

En posant

$$x + y + z = s, \quad x^2 + y^2 + z^2 + xy + yz + zx = u,$$
$$u^2 + xyzs = t, \quad (x+y)(y+z)(z+x) = v,$$

on a

$$s^7 = 7vt.$$

De cette dernière, l'auteur tire $v = 7^6 p^7$, $t = q^{14}$, et, par suite, $u = qr$,

d'où

$$s = 7pq^2, \quad xy + yz + zx = 7^2 p^2 q^4 - qr,$$
$$xyz = 7pq^2(7^2 p^2 q^4 - qr) - 7^6 p^7.$$

La relation $t = q^{14}$ devient

$$q^{12} = r^2 + 7^2 p^2 q^2 (7^2 p^2 q^3 - r) - 7^7 p^8,$$

qui s'écrit

$$\left(r - \frac{1}{2} 7^2 p^2 q^3\right)^2 = q^{12} - 3\left(\frac{1}{2} 7^2 p^2 q^3\right)^2 + 7^7 p^8,$$

c'est-à-dire, en posant

$$p^2 = 2^{a+1} r_1, \quad q_1 = q^3 \quad \text{et} \quad p_1 = r - \frac{1}{2} 7^2 p^2 q^3,$$

$$p_1^2 = q_1^4 - 2^{2a} \,.\, 3 \,.\, 7^4 q_1^2 r_1^2 + 2^{4a+4} \,.\, 7^7 r_1^4,$$

équation impossible d'après le premier théorème.

REMARQUE. — Dans un second article, l'auteur démontre, d'une manière analogue, un cas oublié de décomposition, que Lamé lui avait signalé.

§ V. $x^{2n} + y^{2n} = z^2$, par LEBESGUE (1840).

THÉORÈME. — *Si l'équation* $X^n + Y^n = Z^n$ *est impossible, il en sera de même de l'équation* $x^{2n} + y^{2n} = z^2$.

z doit être impair, car un carré pair ne saurait avoir la forme $4k+2$, qu'aurait le premier membre si x, y étaient impairs. L'équation peut donc s'écrire $(2^a x)^{2n} + y^{2n} = z^2$, x, y, z impairs.

n est pair ou impair. L'auteur traite les deux cas. Pour simplifier, on supposera ici n impair, puisqu'on sait que $x^4 + y^4 = z^2$ est impossible.

Posant $x = pq$, p, q impairs et premiers relatifs, on aura

$$z \pm y^n = 2p^{2n}, \qquad z \mp y^n = 2^{2na-1} q^{2n},$$

et, par suite,

$$z = p^{2n} + 2^{2na-2} q^{2n}, \qquad y^n = p^{2n} - 2^{2na-2} q^{2n}, \qquad y \gtrless 0.$$

Soit $y = rs$, r, s impairs, premiers entre eux, et l'un d'eux négatif si c'est nécessaire.

Il faudra poser $r^n = p^n + 2^{an-1} q^n$, $s^n = p^n - 2^{an-1} q^n$, d'où $r^n - s^n = (2^a q)^n$.

Quel que soit le signe de s, cette dernière équation a toujours la forme $X^n + Y^n = Z^n$. Donc l'impossibilité de celle-ci entraîne celle de $x^{2n} + y^{2n} = z^2$.

§ VI. $Z^{2n} - Y^{2n} = 2x^n$,

par Liouville (1840).

Théorème. — *Si l'équation $u^n + v^n = w^n$ est impossible, $Z^{2n} - Y^{2n} = 2x^n$ l'est également.*

En effet, la première impossibilité entraîne, d'après M. Lebesgue, celle de $x^{2n} + y^{2n} = z^2$. Posons $Y^{2n} + x^n = z$. Il viendrait, si on avait $Z^{2n} - Y^{2n} = 2x^n$, $Z^{2n} - x^n = z$. On trouverait donc à la fois $z - x^n = Y^{2n}$, $z + x^n = Z^{2n}$, d'où, en multipliant membre à membre et faisant pour abréger $YZ = y$, $x^{2n} + y^{2n} = z^2$, qui est impossible.

Donc l'équation proposée $Z^{2n} - Y^{2n} = 2x^n$ est impossible aussi. Elle l'est même pour $n = 2$, puisqu'elle conduit alors à $x^4 + y^4 = z^2$, inadmissible.

§ VII. — Binomes cubiques $x^3 \pm y^3$, par LAMÉ (1865).

Soit $x^3 - y^3$, x, y premiers relatifs. On a

$$x^3 - y^3 = (x-y)\left[\left(\frac{x-y}{2}\right)^2 + 3\left(\frac{x+y}{2}\right)^2\right], \quad x, y, \text{ impairs},$$

$$x^3 - y^3 = (x-y)\left[\left(\frac{x}{2}+y\right)^2 + 3\left(\frac{x}{2}\right)^2\right], \quad x, \text{ pair},$$

$$x^3 - y^3 = 3(x-y)\left[\left(\frac{x+y}{2}\right)^2 + 3\left(\frac{x-y}{2.3}\right)^2\right]$$

ou $\left[\left(\frac{x}{2}\right)^2 + 3\left(\frac{x}{2}+\frac{y-x}{3}\right)^2\right]$, $x-y$ divisible par 3.

Dans tous les cas, $x^3 - y^3 = \delta q$; q, de forme générale a^2+3b^2, est dit le *quadrat* de x^3-y^3.

Le carré du quadrat a^2+3b^2 s'écrit $(a^2-3b^2)^2+3(2ab)^2$, a et $3b$ premiers relatifs. Son cube s'écrit

$$[a(a^2-9b^2)]^2 + 3[3b(a^2-b^2)]^2.$$

L'auteur démontre que tout nombre entier est, de deux manières, la valeur du rapport de deux binomes cubiques. C'est ainsi qu'on a par exemple $2b = \frac{(4b+1)^3+(2b-1)^3}{(2b+2)^3-(2b-1)^3}$; si donc cet entier est un cube, le problème d'Euler se trouve résolu : trouver quatre cubes dont la somme soit nulle.

Il démontre aussi que $x^3+y^3 = Nz^2$ est résoluble d'une infinité de manières et que $x^3+y^3 = Nz^3$ peut être résolue, excepté lorsque N est un cube. L'exception est facilement vérifiable. En effet, pour que N soit un cube, x, y supposés impairs, le δ et le quadrat du premier membre doivent être des cubes. Il en résulte que le δ, pair, sera nécessairement égal à $2a(a^2-9b^2)$ ou à $6b(b^2-a^2)$, suivant que $x+y$ ne sera pas ou sera divisible par 3. Mais, a et $3b$ étant premiers relatifs et de parités différentes, le δ ne peut être un cube que si $a = 4k^3$, $a-3b = i^3$, $a+3b = j^3$ dans le premier cas, ou

$b = 4k^3$, $b - a = i^3$, $b + a = j^3$ dans le second cas, et il faudra que l'on ait, dans les deux cas, $i^3 + j^3 = (2k)^3$, i, j, k étant plus petits que x, y, z ; ce qui conduit à l'impossibilité.

« Cette exception est, en quelque sorte, compensée par la proposition suivante : le produit de deux binomes cubiques peut égaler un cube. »

On obtient une infinité de vérifications :

$$(3^3 + 1^3)(5^3 - 3^3) = 14^3, \qquad (7^3 + 2^3)(8^3 - 7^3) = 39^3.$$

CHAPITRE IX

DE LAMÉ A KUMMER

---

§ I. $A^5 + B^5 + C^5 = 0$, en nombres complexes, par LAMÉ (1847).

La première partie rappelle les propriétés des N. C. relatifs à l'exposant 5 et en signale de nouvelles. La seconde partie démontre l'impossibilité de l'équation.

PREMIÈRE PARTIE. — Soit le N. C.

$$A(r) = a_0 + a_1 r + a_2 r^2 + a_3 r^3 + a_4 r^4,$$

$a_0, a_1, \ldots$ entiers, r racine de $x^5 - 1$.

En particulier, $r + r^4$ ou z_1, $r^2 + r^3$ ou z_2 sont réels, ainsi que $a_0 + a_1 z_1 + a_2 z_2$. $A(r^2)$, $A(r^3)$, $A(r^4)$ sont dits les conjugués de $A(r)$ ou A. On les désigne par A_1, A_2, A_3, A_4. Leur produit est un entier positif et dit la norme de A, $\mathfrak{N}A$; ils sont dits les sous-facteurs de cet entier. En particulier,

$\mathfrak{N}(z_1) = z_1^2 z_2^2 = 1$, $\mathfrak{N}(3 + 2z_i) = 1$, $\mathfrak{N}(r) = 1$, $\mathfrak{N}(1 + r) = 1$.

On remarque que $1 + r = r^3 z_2$.

On reconnaît que $r^k z_1^i$, $r^k z_2^i$ représentent généralement les N. C. de norme unité.

L'auteur établit les propositions suivantes :

Tout N. C., de norme N, ne peut être divisé par un sous-facteur d'un nombre premier n, qui ne diviserait pas N.

Si $\mathfrak{N}(A)$ ou N est premier et si $A = BC$, B a pour norme N et C a pour norme l'unité.

Lorsque A et B ont pour norme un nombre premier N, A est divisible par un conjugué de B, et B par un conjugué de

A; mais A ne peut pas être divisé par un autre conjugué de B, à moins que $N = 5$.

Par suite, les quatre sous-facteurs d'un nombre premier autre que 5 sont premiers entre eux, c'est-à-dire qu'ils ne peuvent avoir d'autre facteur commun que des sous-facteurs de l'unité.

Lorsque $\mathfrak{N}A = m.n$, nombres premiers, dont on connaît deux sous-facteurs respectifs a, b, A est divisible par un des conjugués de a, ensuite par un des conjugués de b, et le quotient définitif a pour norme l'unité. Par suite, si $N = n^\alpha . m^\beta \ldots$, A sera le produit d'un sous-facteur de l'unité par α sous-facteurs, égaux à un ou à plusieurs des conjugués de a, sous-facteur de n, par β sous-facteurs, etc.

Ainsi, pour décomposer A en ses facteurs premiers, on essaiera successivement α fois la division par les conjugués de a, et l'on réussira à toutes les fois; ensuite on procédera aux β divisions, etc. Le quotient définitif aura pour norme l'unité.

De là et de ce qu'un N. C. ne peut être divisible par un sous-facteur d'un nombre premier qui ne divise pas sa norme, on conclura aisément qu'un N. C. ne peut être divisible que d'une seule manière en ses facteurs premiers.

On a

$$A^5 + B^5 = (A + B)(Ar + Br^4)(Ar^2 + Br^3)(Ar^3 + Br^2)(Ar^4 + Br).$$

Les facteurs du second membre, M, M', ... vérifient les trois équations

$$M'' + M''' = \varepsilon_h M', \qquad M^{IV} + M = \varepsilon_h M'', \qquad M' + M'' = \varepsilon_h M^{IV}.$$

Il en résulte qu'un N. C. dont la norme n'est pas l'unité ne peut diviser deux des cinq facteurs sans les diviser tous.

DEUXIÈME PARTIE. — Soit $A^5 + B^5 + C^5 = 0$, A, B, C premiers entre eux.

L'auteur démontre, à l'aide de

$$(A + B + C)^5 = 5(A + B)(B + C)(C + A)\,[(A + B + C)^2 - (AB + BC + CA)],$$

que C, par exemple, est divisible par $1 - r$ ou λ.

C'est aussi la condition pour que les équations

$$A^5 + B^5 = z_h^2 C^5, \qquad A^5 + B^5 = z_h C^5, \qquad h = 1, 2,$$

soient possibles ; en tout, cinq équations (E).

Dans ces équations, C est divisible par λ_1^2, et, par suite, $A^5 + B^5$ par λ_1^{10}. On en déduit la composition des M : $M = \nu\mu^5$, $M' = \nu'\mu'^5$, ... ; les ν ont la forme $r^k z_h^i$, l'un d'eux, ν^{IV} est égal à 1.

Substituant ces valeurs des M dans les équations ci-dessus, on obtient trois équations telles que $\nu'''\mu'''^5 + \mu^{IV5} = z_h \nu' \mu'^5$. Il reste à réduire les ν. On trouve qu'ils se réduisent à des puissances de z_h et qu'ils ne contiennent pas de facteur r.

On trouve ainsi qu'une équation au moins sur les trois se réduit à la forme $m''^5 + m'''^5 = z_h^j m'^5$, $j = 1$, 2 (e). Alors, si l'équation (e) est semblable à celle des (E), d'où l'on est parti, l'impossibilité de l'équation proposée sera établie de suite, puisqu'une solution supposée de cette équation conduit à une solution en nombres beaucoup plus petits, la grandeur d'un N. C. se mesurant par celle de sa norme.

Si, au contraire, e est semblable à une autre E, on traitera de nouveau cette seconde équation e, qui conduira à une troisième de la même forme générale.

Si cette troisième est semblable à la deuxième ou à la première, leur impossibilité est établie ; si elle est encore différente, on en déduira une quatrième.

En continuant ainsi, on retombera, après cinq transformations au plus, sur une équation semblable à l'une de celles qui la précèdent ; d'où résultera leur impossibilité.

§ II. $A^m + B^m + C^m = 0$, par Lamé.

Démonstration analogue.

§ III. — **Mémoires de Cauchy** (1839, 1847).

Cauchy appelle polynomes radicaux les N. C. formés avec les racines primitives de $x^n = 1$; factorielle, la norme ;

équivalences, les congruences. Voici quelques titres de ces mémoires : Sur de nouvelles formules relatives aux polynomes radicaux et sur le théorème de Fermat ; sur les plus petites factorielles qui correspondent à un polynome radical ; sur la décomposition d'un polynome radical en deux parties, dont l'une corresponde à une factorielle plus petite que l'unité ; sur la décomposition d'un entier en facteurs radicaux ; sur les facteurs modulaires des fonctions entières d'une ou de plusieurs variables ; sur les indices modulaires des polynomes radicaux.

« Lorsqu'on veut faire servir à la démonstration du théorème de Fermat la considération des polynomes radicaux, on a deux problèmes à résoudre ; d'abord, on doit faire voir qu'un produit de polynomes radicaux ne peut être décomposé que d'une seule manière, et c'est le plus important, puisque, en supposant ce principe établi, on peut en déduire le théorème de Fermat.

« Je commencerai à m'occuper du premier. Après quelques recherches, je suis parvenu à le ramener à une question de maximum, ainsi qu'on le verra dans ce Mémoire sur la décomposition d'un polynome en deux parties dont l'une correspond à une factorielle plus petite que l'unité. »

Enfin, le 26 juillet : « ... Dans un prochain article, j'expliquerai comment ces diverses propositions peuvent servir à la démonstration du théorème de Fermat », et le 2 août : « ... de ces propositions, on peut déjà déduire diverses conséquences relatives à la démonstration du théorème de Fermat. Il en résulte, par exemple, que, pour démontrer la relation $a^n + b^n + c^n = 0$, en nombres entiers, premiers à n, il suffit de s'assurer que la somme

$$1 + 2^{n-4} + 3^{n-4} + \cdots + \left(\frac{n-1}{2}\right)^{n-4}$$

n'est pas divisible par n. »

Cauchy n'en donne aucune raison. Quant à la somme elle-même, comment vérifier l'exactitude des puissances calculées ? Pour $n = 67$, 7^{63} renferme 54 chiffres ; que serait-ce pour 33^{63} ?

§ IV. — Mémoire sur la théorie des nombres complexes, par E. Kummer (1849-50).

Nombre complexe :

$$f(\alpha) = a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{\lambda-1}\alpha^{\lambda-1},$$

où α est racine primitive de $x^\lambda - 1 = 0$; λ, premier, les coefficients, entiers. Le produit $f(\alpha)f(\alpha^2)\ldots f(\alpha^{\lambda-1})$ est un nombre entier, désigné par $Nf(\alpha)$, norme de $f(\alpha)$. Exemple :

$$(1-\alpha)(1-\alpha^2)\ldots(1-\alpha^{\lambda-1}) = \lambda.$$

Suivant que $a_0 + a_1 + \ldots + a_{\lambda-1}$ n'est pas ou est multiple de λ, $Nf(\alpha) \equiv 1$ ou $0 \pmod{\lambda}$.

Unité complexe : tout nombre complexe dont la norme est égale à 1 ; désignée par $E(\alpha)$.

Unités simples : $\pm 1, \pm\alpha, \ldots \pm\alpha^{\lambda-1}$. Le nombre des autres est infini. Exemple : $\frac{1-\alpha^r}{1-\alpha}$, $r < \lambda$. $E(\alpha)$ et $E(\alpha^{-1})$ sont dites réciproques. On démontre que $E(\alpha^{-1}) = \pm\alpha^m E(\alpha)$.

On considère aussi des fonctions entières de deux racines ; $\alpha + \alpha^{\lambda-1}$, $\alpha^2 + \alpha^{\lambda-2}$ sont dites unités fondamentales.

Si p est premier, $p = Nf(\alpha)$; $f(\alpha)$, $f(\alpha^2)$ ... sont des nombres complexes premiers, parce qu'on ne peut pas avoir $f(\alpha) = \varphi(\alpha)\psi(\alpha)$, à moins que l'un des facteurs soit une unité complexe.

On démontre que tous les nombres complexes sont congrus à des nombres réels pour le module $f(\alpha)$, dont la norme est un nombre premier. On démontre ensuite que tous les nombres complexes de même norme qui est un nombre premier, ne diffèrent pas entre eux, si ce n'est par des unités complexes, par lesquelles ils peuvent être multipliés.

Des périodes des racines de l'équation $1 + \alpha + \cdots + \alpha^{\lambda-1} = 0$ *et de leur correspondance avec les racines des congruences analogues.*

« Passons maintenant à la discussion des nombres complexes dont les normes sont des entiers quelconques.

« Soit $\lambda - 1 = ef$, γ une racine primitive de la congruence $\gamma^{\lambda-1} \equiv 1$ (mod. λ). Les racines peuvent être rangées en e périodes de f termes : α, α^{γ}, α^{γ^2}, ... $\alpha^{\gamma^{e-1}}$, α^{γ^e}, ... $\alpha^{\gamma^{2e-1}}$ ... $\alpha^{\gamma^{ef-1}}$.

« Périodes η, η_1, ... η_{e-1}. $\eta = \alpha + \alpha^{\gamma^e} + \alpha^{\gamma^{2e}} + \cdots + \alpha^{\gamma^{(f-1)e}}$,

$$\eta_1 = \alpha^{\gamma} + \alpha^{\gamma^{e+1}} + \cdots + \alpha^{\gamma^{(f-1)e+1}},$$

. . . .

« En faisant le produit de deux périodes, on obtient e équations fondamentales telles que

$$\eta\eta_1 = nf + m\eta + m_1\eta_1 + \cdots + m_{e-1}\eta_{e-1},$$

et on déduit de ce système une équation à coefficients entiers, dont les racines sont les e périodes.

« On démontre que cette équation, prise pour congruence pour un module q, nombre premier satisfaisant à la condition $q^f \equiv 1$ (mod. λ), a toujours e racines réelles.

« Cela étant, nous établissons un système de congruences parfaitement analogues aux équations fondamentales, telles que $uu_1 \equiv nf + mu + m_1u_1 + \cdots + m_{e-1}u_{e-1}$ (mod. q) et on déduit de ce système une congruence parfaitement analogue à l'équation dont les racines sont les périodes, de laquelle on tirera les valeurs réelles de u, u_1 ... u_{e-1}. »

De la conformité des équations et des congruences, l'auteur déduit que toute équation qui ne contient que des fonctions rationnelles et entières des périodes donne immédiatement une congruence quand on y remplace les périodes par les entiers correspondants. Exemple : $\eta + \eta_1 + \cdots + \eta_{e-1} = -1$ (somme des α) donne $u + u_1 + \cdots + u_{e-1} \equiv -1$ (mod. q).

Des facteurs premiers de la norme d'un nombre complexe quelconque.

« Un nombre complexe contenant les périodes peut être considéré comme fonction d'une seule période, η par exemple ; aussi nous le désignerons par $F(\eta)$. De même, le nombre entier qui en résulte si on remplace les périodes par les racines des congruences sera désigné par $F(u)$. »

L'auteur démontre deux théorèmes : Si un nombre complexe contenant des périodes est divisible par q, premier, satisfaisant à la congruence $q^f \equiv 1 \pmod{\lambda}$, tous les entiers qu'on déduit de ce nombre complexe en remplaçant les périodes par les racines des congruences analogues sont divisibles par q, et réciproquement. — Si la norme d'un nombre complexe $F(\eta)$ est divisible par q, un des nombres $F(u)$, $F(u_1)$, ... $F(u_{e-1})$ sera divisible par q, et réciproquement.

« Nous allons maintenant discuter les conditions nécessaires pour que la norme d'un nombre complexe quelconque, composé des racines α, ait un facteur premier donné q, satisfaisant à $q^f \equiv 1 \pmod{\lambda}$, et, de plus *appartenant à l'exposant f*, c'est-à-dire tel qu'aucune autre puissance de q, inférieure à la $f^{ième}$, ne soit congrue à 1. »

L'auteur aboutit à ce théorème : Si $Nf(\alpha)$ est divisible par q, il faut que les f congruences $\varphi(u_r) \equiv 0$, $\varphi_1(u_r) \equiv 0$, ... $\varphi_{f-1}(u_r) \equiv 0 \pmod{q}$, qu'on obtient en mettant $f(\alpha)$ sous la forme

$$f(\alpha) = \varphi(\eta) + \alpha\varphi_1(\eta) + \cdots + \alpha^{f-1}\varphi_{f-1}(\eta),$$

et remplaçant les e périodes par les racines des congruences correspondantes, aient lieu pour une certaine valeur de r et réciproquement.

Définition et propriétés générales des facteurs idéaux d'un nombre complexe.

« D'après ce qui précède, nous sommes en état d'assigner tous les nombres complexes dont les normes ont un facteur premier donné. Y en a-t-il dont la norme soit égale à ce nombre premier ?

« D'abord, nous savons que quand $Nf(\alpha)$ est divisible par q, premier, appartenant à l'exposant f, elle ne peut pas être égale à q, à moins que $f = 1$, c'est-à-dire à moins que q, appartenant à l'exposant 1, n'ait la forme $m\lambda + 1$.

« Mais parmi les nombres complexes contenant les périodes

à f termes, il pourra y en avoir dont les normes, prises par rapport aux périodes, soient égales à q. Donc il se pourra qu'un nombre q soit décomposable en e facteurs conjugués, de sorte qu'on ait $\varphi(\eta)\varphi(\eta_1)\ldots\varphi(\eta_{e-1})=q$, et, en particulier pour le cas de $f(x)$, il se pourra qu'un nombre premier de la forme $m\lambda+1$ soit tel qu'on ait $f(\alpha)f(\alpha^2)\ldots f(\alpha^{\lambda-1})=p$.

« Par suite, on divisera tous les nombres premiers en deux classes, suivant qu'ils peuvent ou ne peuvent pas être représentés comme normes.

« *Première classe.* — Pour distinguer les facteurs premiers de q, premier, nous ferons usage des nombres $u, u_1 \ldots u_{e-1}$, correspondant aux périodes. En les substituant, on aura, pour une certaine valeur de r, $\varphi(u_r)\equiv 0$ (mod. q), condition nécessaire pour que la norme de $\varphi(\eta)$ soit divisible par q. On voit par là que, pour les divers facteurs premiers de q, on a $\varphi(\eta)\equiv 0$ pour $\eta=u_r$, $\varphi(\eta_1)\equiv 0$ pour $\eta=u_{r-1}$, et généralement $\varphi(\eta_k)\equiv 0$ pour $\eta=u_{r-k}$.

« Nous distinguons donc les e facteurs premiers conjugués de q selon les racines des congruences qui doivent être choisies comme correspondantes aux périodes pour que chacun de ces facteurs premiers complexes soit congru à zéro par rapport au module q.

« Nous voyons par là que la condition $F(x)\equiv 0$ (mod. q) pour $\eta=u_r$ définit complètement un facteur premier complexe $\varphi(\eta)$, contenu dans le nombre $F(x)$, toutes les fois que le nombre premier $\varphi(\eta)$ *existe* réellement, c'est-à-dire quand q est de première classe.

« *Seconde classe.* — On ne peut plus isoler un facteur premier d'un nombre complexe $f(\alpha)$, satisfaisant à la condition $f(x)\equiv 0$ (mod. q), pour $\eta=u_r$.

« Nous dirons néanmoins que ce nombre complexe contient un facteur premier complexe du nombre q, que nous appellerons facteur premier *idéal* de q, et, puisque nous avons vu que les e facteurs du nombre premier, s'ils existent effectivement, sont distingués en ce que chacun d'eux devient congru à zéro pour une certaine substitution des racines de

congruences au lieu des périodes, nous désignerons ce facteur premier idéal de q comme appartenant à la substitution $\eta = u_r$.

« Les nombres complexes idéaux seront opposés aux nombres complexes existants comme, en algèbre, les nombres imaginaires sont opposés aux nombres réels. »

L'auteur ajoute : « Nous allons démontrer les théorèmes élémentaires pour le calcul des facteurs idéaux, qui sont entièrement les mêmes que pour les facteurs existants. »

Voici le dernier : Lorsqu'une puissance d'un nombre complexe est décomposée en plusieurs facteurs premiers entre eux, ces facteurs seront séparément des puissances semblables multipliées par des unités complexes.

De la composition des nombres idéaux.

« La norme d'un nombre idéal sera toujours un nombre existant ; car, en supposant que $f(\alpha)$ contient m facteurs idéaux de l'entier q, appartenant à l'exposant f, de même m' facteurs idéaux de q', appartenant à f', etc., la norme $Nf(\alpha)$, contenant tous les facteurs idéaux de q, q' ..., sera divisible par q^{mf} $q'^{m'f'}$ ..., et, puisqu'elle ne contient pas d'autres facteurs idéaux, elle sera égale à q^{mf} $q'^{m'f'}$ ... à une unité près.

« Le problème de trouver un nombre complexe existant $F(\alpha)$, qui ait le facteur idéal $f(\alpha)$, aura toujours une infinité de solutions, c'est-à-dire il y aura toujours une infinité de nombres idéaux qui, multipliés par le nombre idéal $f(\alpha)$, produisent des nombres existants. Ils sont nommés *nombres idéaux équivalents*. Ils forment une *classe* de nombres idéaux ; il y a un nombre fini de classes, chaque nombre idéal appartient à une seule classe.

« Tout nombre complexe idéal, élevé à une certaine puissance entière, donne un nombre complexe existant ; l'exposant de cette puissance a un diviseur commun avec le nombre des classes de tous les nombres idéaux. »

Recherche du nombre H *de classes des nombres complexes idéaux.*

L'auteur calcule de deux manières $\Sigma \frac{s-1}{N(f(\alpha))^s}$, le signe sommatoire étant pris par rapport à tous les nombres complexes, existants et idéaux. Dans la seconde manière, il les distingue les uns des autres, et aussi les H classes des idéaux les unes des autres, depuis $(f(\alpha))^s$ jusqu'à $(f_{H-1}(\alpha))^s$. Comme toutes ces sommes particulières sont égales, le calcul fait apparaître H.

Il ne reste qu'à égaler les expressions trouvées dans les deux manières. Il trouve $H = \frac{P}{(2\lambda)^{\frac{\lambda-3}{2}}} \times \frac{D}{\Delta}$ et prouve que les deux facteurs sont entiers.

« Le calcul du second est très pénible quand λ croît. J'ai calculé le premier pour tous les nombres premiers de la première centaine ; ses valeurs croissent avec une rapidité extraordinaire. Pour $\lambda = 37, 59, 67$, il est égal à

$$37, \quad 3.59.233, \quad 67.12739. \text{ »}$$

Deux recherches spéciales concernant le nombre des classes et les unités complexes.

La première consiste à trouver tous les nombres premiers λ pour lesquels le premier facteur de H est divisible par λ.

Il démontre que cette divisibilité dépend d'une congruence à vérifier, qui contient des sommes telles que

$$1 + 2^{2n-1} + 3^{2n-1} + \ldots + (x-1)^{2n-1}.$$

On sait que cette somme s'exprime ainsi

$$(2n-1)!\left\{\frac{x^{2n}}{2n!} - \frac{x^{2n-1}}{2.(2n-1)!} + \frac{B_1 x^{2n-2}}{(2n-2)!\,2!} - \frac{B_2 x^{2n-4}}{(2n-4)!\,4!} + \cdots + (-1)^n \frac{B_{n-1} x^2}{2!(2n-2)!}\right\},$$

de sorte que la congruence finit par se réduire à

$$B_n \equiv 0 \pmod{\lambda}.$$

Le second facteur de H, rapport de deux déterminants formés d'unités complexes, ne sera divisible par λ que si le premier l'est.

Et voici la conclusion : *Pour que le nombre* **H** *soit divisible par* λ, *il faut et il suffit que* λ, *premier, divise le numérateur d'un quelconque des* $\frac{\lambda-3}{2}$ *premiers nombres bernoulliens.*

La seconde recherche aboutit à ce théorème : *Si* λ, *premier, n'est contenu dans aucun des* $\frac{\lambda-3}{2}$ *premiers nombres bernoulliens, comme facteur du numérateur, toute unité complexe congrue à un nombre entier non complexe pour le module* λ, *sera une* $\lambda^{ième}$ *puissance d'une autre unité complexe.*

Démonstration générale du théorème de Fermat.

Théorème. — *L'équation* $u^\lambda + v^\lambda + w^\lambda = 0$ *est insoluble en nombres entiers pour tous les exposants premiers impairs* λ *qui ne figurent pas comme facteurs dans les numérateurs des* $\frac{\lambda-3}{2}$ *premiers nombres de Bernoulli.*

Rappelons qu'en supposant $f(\alpha)$ idéal, $(f(\alpha))^\lambda$ ne pourra être existant, λ étant supposé tel qu'il a été dit.

Soit donc $$u^\lambda + v^\lambda + w^\lambda = 0 \qquad (1)$$
la relation à examiner ; u, v, w désignant des nombres complexes existants de la forme

$$a_0 + a_1\alpha + a_2\alpha^2 + \ldots + a_{\lambda-2}\alpha^{\lambda-2},$$

et premiers entre eux deux à deux.

Première partie : *aucun des nombres* u, v, w *ne contient le facteur* $1-\alpha$.

Comme dans l'équation ne figurent que les puissances $\lambda^{ièmes}$ de u, v, w, on peut les multiplier par une unité simple sans que l'équation change de forme. On pourra donc écrire $\alpha^k u$

au lieu de u, où k est un entier quelconque, qui peut toujours être déterminé de manière que $\alpha^k u$ acquière la forme $a + (1 - \alpha)^2 P$, où a est un entier réel et P un nombre entier complexe.

En effet, le nombre complexe u, ordonné suivant les puissances de $1 - \alpha$, prend la forme

$$u = A + A_1(1 - \alpha) + A_2(1 - \alpha)^2 + \ldots + A_{\lambda-2}(1 - \alpha)^{\lambda-2}.$$

De même, en prenant $\alpha = 1 - (1 - \alpha)$, on aura

$$\alpha^k = 1 - k(1 - \alpha) + \frac{k(k-1)}{1 \cdot 2}(1 - \alpha)^2 \ldots,$$

d'où, en multipliant et comprenant dans un seul terme les termes multipliés par $(1 - \alpha)^2$,

$$\alpha^k u = A + (A_1 - Ak)(1 - \alpha) + (1 - \alpha)^2 P.$$

Enfin, en prenant le nombre k tel qu'on ait $Ak \equiv A_1 \pmod{\lambda}$, ce qui est toujours possible puisque A n'est pas divisible par λ, on voit que $\alpha^k u$ prend la forme proposée.

On prendra donc

$$u = a + (1 - \alpha)^2 P, \quad v = b + (1 - \alpha)^2 Q, \quad w = c + (1 - \alpha)^2 R.$$

Les entiers réels a, b, c ne sont pas (en vertu de la condition que u, v, w ne sont pas divisibles par $1 - \alpha$) divisibles par λ.

Je décompose maintenant la forme $u^\lambda + v^\lambda$ en ses facteurs et j'ai

$$(u + v)(u + \alpha v)(u + \alpha^2 v) \ldots (u + \alpha^{\lambda-1} v) = - w^\lambda. \quad (3)$$

Ces λ facteurs n'ont pas de diviseur commun ; car, si $u + \alpha^r v$ et $u + \alpha^s v$ en avaient un, $(\alpha^r - \alpha^s)u$ et $(\alpha^r - \alpha^s)v$ devraient avoir le même diviseur, et, comme u et v sont premiers entre eux, ce diviseur serait $\alpha^r - \alpha^s$. Mais $\alpha^r - \alpha^s$ est égal à $1 - \alpha$ multiplié par une unité complexe, et celle-ci ne peut être diviseur de l'un des λ facteurs, parce que, autrement, contre l'hypothèse, également w^λ, et par suite également w, devrait être divisible par $1 - \alpha$.

Comme, maintenant, ces λ facteurs n'ont pas de diviseur commun, deux à deux, et comme leur produit est égal à une puissance $\lambda^{ième}$, ils doivent être tous égaux séparément aux puissances $\lambda^{ièmes}$ de nombres complexes idéaux, multipliés par des unités complexes.

Une conséquence immédiate est (en vertu du théorème démontré t. XXXV, p. 348) : tout comme les nombres entiers ordinaires, abstraction faite des unités qui peuvent entrer comme facteurs, chaque nombre complexe ne se présente que d'une seule manière déterminée comme produit de ses facteurs premiers idéaux.

On obtient alors d'une manière générale pour toutes les valeurs de r, 0, 1, 2, ..., $\lambda - 1$,

$$u + \alpha^r v = \alpha^q \,.\, E_r(\alpha) t_r^\lambda, \tag{4}$$

où t est un nombre complexe facteur de w, et $\alpha^q E_r(\alpha)$ une unité complexe quelconque dans laquelle $E_r(\alpha) = E_r(\alpha^{-1})$.

Chaque unité complexe se partage, comme c'est connu, en deux facteurs α^q et $E_r(\alpha)$, dont l'un est seulement une racine $\lambda^{ième}$ de l'unité, et l'autre a la propriété de rester inchangé par la transformation de α en α^{-1}.

Comme, d'après l'équation (4), t_r^λ est égal à un nombre complexe existant, nous en concluons aussitôt, d'après ce que nous avons démontré plus haut, que t_r lui-même également doit être un nombre complexe existant, et, comme chaque puissance $\lambda^{ième}$ d'un nombre complexe est, comme c'est connu, congrue à un nombre entier réel pour le module λ, je pose $t_r^\lambda \equiv m$ (mod. λ), où m est un nombre entier réel. Par cela l'équation (4) se transforme en la congruence

$$u + \alpha^r v \equiv \alpha^q E_r(\alpha) \,.\, m \quad (\text{mod. } \lambda). \tag{5}$$

Maintenant, si on change α en α^{-1}, par quoi u, v, w en u', v', w', nombres complexes réciproques de u, v, w, on a

$$u' + \alpha^{-r} v' \equiv \alpha^q E_r(\alpha) \,.\, m \quad (\text{mod. } \lambda). \tag{6}$$

De ces deux congruences on obtient par élimination

de m

$$\alpha^{-q}(u+\alpha^r v) \equiv \alpha^q(u'+\alpha^{-r}v'), \quad (\text{mod. } \lambda). \qquad (7)$$

Si on prend, au lieu de mod. λ, le module $(1-\alpha)^2$, qui est un diviseur de λ, et si on remarque que, d'après l'égalité (2),

$$u \equiv a, \quad v \equiv b, \quad u' \equiv a, \quad v' \equiv b \quad [\text{mod. } (1-\alpha)^2],$$

on obtient

$$\alpha^{-q}(a+\alpha^r b) \equiv \alpha^q(a+\alpha^{-r}b) \; [\text{mod. } (1-\alpha)^2] \qquad (8)$$

et, comme généralement $\alpha^h \equiv 1 - h(1-\alpha)$ [mod. $(1-\alpha)^2$]. cette congruence se transforme en la suivante

$$2(a+b)q \equiv 2br \; [\text{mod. } (1-\alpha)].$$

Comme maintenant les nombres entiers réels, qui sont divisibles par $1-\alpha$, doivent être également divisibles par λ, on a

$$(a+b)q \equiv br \; (\text{mod. } \lambda). \qquad (9)$$

Si on appelle k l'entier qui satisfait à la congruence

$$(a+b)k \equiv r \; (\text{mod. } \lambda), \qquad (10)$$

k est indépendant de r et $q \equiv kr$; ainsi la congruence (7) donne

$$\alpha^{-kr}(u+\alpha^r v) \equiv \alpha^{kr}(u'+\alpha^{-r}v') \; (\text{mod. } \lambda). \qquad (11)$$

Pour le cas particulier où $r=0$, puisqu'on ne peut avoir $a+b \equiv 0$ (mod. λ), de la congruence (9) on tire

$$q \equiv 0 \; (\text{mod. } \lambda).$$

On a également

$$u+v \equiv u'+v' \; (\text{mod. } \lambda), \qquad (12)$$

et, comme dans $u^\lambda + v^\lambda + w^\lambda = 0$, u, v, w peuvent être intervertis à volonté, on a également

$$u+w \equiv u'+w', \quad v+w \equiv v'+w' \; (\text{mod. } \lambda) \qquad (13)$$

et de ces congruences découlent les trois plus simples

$$u \equiv u', \qquad v \equiv v', \qquad w \equiv w' \qquad (\text{mod. } \lambda). \qquad (14)$$

D'après cela, la congruence (11), valable pour chaque valeur de r, se transforme en la suivante

$$\alpha^{-kr}(u + a^r v) \equiv \alpha^{kr}(u + \alpha^{-r} v) \pmod{\lambda}, \qquad (15)$$

ou en

$$u(\alpha^{kr} - \alpha^{-kr}) + v(\alpha^{(k-1)r} - \alpha^{-(k-1)r}) \equiv 0 \pmod{\lambda}.$$

Faisant dans cette dernière $r = 1$ et $r = 2$, on obtient

$$\begin{aligned} &u(\alpha^k - \alpha^{-k}) + v(\alpha^{k-1} - \alpha^{-(k-1)}) \equiv 0, \\ &u(\alpha^{2k} - \alpha^{-2k}) + v(\alpha^{2(k-1)} - \alpha^{-2(k-1)}) \equiv 0. \pmod{\lambda} \end{aligned} \qquad (16)$$

Et, si on multiplie la première par $\alpha^k + \alpha^{-k}$, et si on en retranche la deuxième, après enlèvement du facteur v, qui n'est pas divisible par $1 - \alpha$ et est également premier à λ, nous obtenons

$$(\alpha^k + \alpha^{-k})(\alpha^{k-1} - \alpha^{-(k-1)}) + \alpha^{2(k-1)} - \alpha^{-2(k-1)} \equiv 0 \pmod{\lambda}$$

et

$$(\alpha^{k-1} - \alpha^{-(k-1)})(\alpha^k + \alpha^{-k} - \alpha^{k-1} - \alpha^{-(k-1)}) \equiv 0$$

et par suite

$$(\alpha^{k-1} - \alpha^{-(k-1)})(\alpha^{-k} - \alpha^{k-1})(1 - \alpha) \equiv 0 \pmod{\lambda}. \qquad (17)$$

Maintenant, si aucun de ces trois facteurs n'est nul par lui-même, leur produit contient trois fois le facteur $1 - \alpha$; mais, pour être divisible par λ, il fallait qu'il contînt ce facteur $\lambda - 1$ fois afin que la congruence ait réellement lieu.

Donc, à l'exception du seul cas $\lambda = 3$, que nous excluons, la congruence (17) ne peut avoir lieu que si on a

$$\alpha^{k-1} - \alpha^{-(k-1)} = 0, \qquad \text{ou} \qquad \alpha^{-k} - \alpha^{k-1} = 0.$$

On doit avoir alors

$$\text{ou bien} \quad k \equiv 1 \quad \text{ou bien} \quad 2k \equiv 1 \pmod{\lambda}.$$

Mais $k \equiv 1$ donnerait, en vertu de la congruence (10), $a \equiv 0 \pmod{\lambda}$, ce qui est contre l'hypothèse, et ne peut par conséquent avoir lieu.

Le second cas donnerait, en vertu de la congruence (10), $a \equiv b$ (mod. λ), d'où il suit par simple changement de lettres (comme conséquence nécessaire de l'équation

$$u^\lambda + v^\lambda + w^\lambda = 0$$

en supposant qu'aucun de u, v, w ne soit divisible par $1 - \alpha$) de u, v, w, ce qui change a, b, c en même temps, que aussi $a \equiv c$, $b \equiv c$ (mod. λ).

Mais de l'équation $u^\lambda + v^\lambda + w^\lambda = 0$, il suit, d'après les expressions prises pour u, v, w (2), qu'on doit avoir également $a^\lambda + b^\lambda + c^\lambda \equiv 0$ (mod. λ) ; donc également $a + b + c \equiv 0$ (mod. λ). En effet, en développant la $\lambda^{ième}$ puissance de $u = a + (1 - \alpha)^2 P$ et en négligeant les termes divisibles par λ, on obtient $u^\lambda \equiv a^\lambda \equiv a$ (mod. λ). De même $v^\lambda \equiv b$, $w^\lambda \equiv c$, et par suite $u^\lambda + v^\lambda + w^\lambda \equiv a + b + c$.

Et, comme a, b, c sont congrus entre eux, on en déduirait $3a \equiv 0$ (mod. λ), qui, à l'exception du cas déjà exclu $\lambda = 3$, est également impossible parce que, par hypothèse, u ne contient pas le facteur $1 - \alpha$, et ainsi ne peut aussi être divisible par λ.

La première partie de la démonstration est ainsi donnée complètement, puisqu'il a été démontré que l'équation $u^\lambda + v^\lambda + w^\lambda = 0$ entraîne toujours une congruence impossible pour le module λ, si aucun des nombres complexes u, v, w ne contient le facteur $1 - \alpha$, à l'exception du cas $\lambda = 3$, que nous ne voulons pas considérer ici.

DEUXIÈME PARTIE : *w est supposé divisible par* $1 - \alpha$.

w peut le contenir plusieurs fois ; à la place de w on écrira donc $(1 - \alpha)^m w$, d'où l'équation

$$u^\lambda + v^\lambda + (1 - \alpha)^{m\lambda} w^\lambda = 0.$$

Je préfère étudier l'équation plus générale

$$u^\lambda + v^\lambda = E(\alpha)(1 - \alpha)^{m\lambda} w^\lambda, \qquad (19)$$

où $E(\alpha)$ est une unité complexe quelconque.

On l'écrit

$$(u+v)(u+\alpha v)\dots(u+\alpha^{\lambda-1}v)=E(\alpha)(1-\alpha)^{m\lambda}w^{\lambda}. \quad (20)$$

Les λ facteurs, premiers deux à deux, ont, tous, le facteur $1-\alpha$. En faisant de nouveau $u=a+(1-\alpha)^2P$, on aura

$$u+\alpha^r v\equiv a+b-rb(1-\alpha) \quad [\text{mod. } (1-\alpha)^2]. \quad (21)$$

Mais $u+\alpha^r v$ doit être, au moins pour une valeur de r, divisible par $(1-\alpha)$, puisque le produit de tous ces facteurs est divisible par $(1-\alpha)^{m\lambda}$; de sorte que $a+b$ doit être divisible par $1-\alpha$, et, par suite aussi, par λ, et la congruence (21) se transforme en

$$u+\alpha^r v\equiv rb(1-\alpha) \quad [\text{mod. } (1-\alpha)^2], \quad (22)$$

d'où il suit que, pour chaque valeur de r, $u+\alpha^r v$ doit contenir le facteur $1-\alpha$, à la place duquel on peut prendre aussi le facteur $1-\alpha^r$, qui ne se distingue de lui que par une unité complexe qui y entre comme facteur ; ensuite, que $u+\alpha^r v$ ne peut contenir qu'une seule fois le facteur $1-\alpha^r$ ou $1-\alpha$, excepté le cas de $r=0$, où l'on a

$$u+v\equiv 0 \quad [\text{mod. } (1-\alpha)^2].$$

Cela étant, il suit immédiatement de l'équation (20) que $u+v$ contient $(m\lambda-\lambda+1)$ fois précisément le facteur $1-\alpha$. On pourra donc poser

$$u+v=(1-\alpha)^{m\lambda-\lambda+1}\varphi \quad (23), \qquad u+\alpha^r v=(1-\alpha^r)\varphi_r \quad (24)$$

et (20) devient

$$\varphi\varphi_1\varphi_2\dots\varphi_{\lambda-1}=E(\alpha)w^{\lambda}. \quad (25)$$

Les nombres complexes φ, $\varphi_1\dots$ sont premiers entre eux deux à deux, car tout facteur commun de φ_r et de φ_s ou de $u+\alpha^r v$ et $u+\alpha^s v$ diviserait également

$$(\alpha^r-\alpha^s)u, \qquad (\alpha^r-\alpha^s)v,$$

dont le p. g. c. d. est $1-\alpha$.

De là on conclut, pour la même raison que dans la pre-

mière partie, que φ, φ_1 ... seront séparément des puissances de degré λ, multipliées par des unités.

On posera donc $\varphi = e_0(x)w_1^\lambda$, $\varphi_r = e_r(\alpha)t_r^\lambda$, ce qui donne

$$u + v = e_0(x)(1 - x)^{m\lambda - \lambda + 1}w_1^\lambda, \tag{26}$$
$$u + x^r v = e_r(x)(1 - x^r)t_r^\lambda. \tag{27}$$

Les nombres complexes w_1, t_r ne sont ici que des nombres existants, parce que leurs puissances $\lambda^{ièmes}$ sont des nombres existants.

On aura aussi

$$u + x^s v = e_s(x)(1 - \alpha^s)t_s^\lambda. \tag{28}$$

Éliminant u, v entre les trois dernières équations, on trouve

$$e_r(x)t_r^\lambda - e_s(x)t_s^\lambda = \frac{e_s(x^r - \alpha^s)(1 - x)}{(1 - \alpha^r)(1 - \alpha^s)}(1 - \alpha)^{(m-1)\lambda}w_1^\lambda. \tag{29}$$

Lorsqu'on y fait, pour abréger,

$$\frac{e_s(x)}{e_t(x)} = -\varepsilon(x), \qquad \frac{e(x)(\alpha^r - x^s)(1 - x)}{e_r(x)(1 - \alpha^r)(1 - x^s)} = \mathrm{E}_1(\alpha)$$

où $\varepsilon(x)$, $\mathrm{E}_1(\alpha)$ sont des unités, on aura

$$t_r^\lambda + \varepsilon(\alpha)t_s^\lambda = \mathrm{E}_1(x)(1 - x)^{(m-1)\lambda}w_1^\lambda. \tag{30}$$

Les nombres complexes t_r, t_s, w_1, dont les puissances sont données comme nombres existants, doivent être eux-mêmes des nombres existants ; leurs $\lambda^{ièmes}$ puissances seront donc congrues à des entiers non complexes pour le module λ, et on aura $t_r^\lambda \equiv k$, $t_s^\lambda \equiv k'$ (mod. λ), et, comme la puissance $(1 - x)^{(m-1)\lambda}$ est divisible par λ si $m > 1$, l'équation (30) donne la congruence $k + \varepsilon(x)k' \equiv 0$ (mod. λ).

En déterminant le nombre c par la congruence

$$k + ck' \equiv 0,$$

on aura $\varepsilon(x) \equiv c$ (mod. λ), et l'unité $\varepsilon(\alpha)$, congrue à un nombre entier non complexe pour le module λ, doit être égale à une $\lambda^{ième}$ puissance d'une autre unité.

Donc, en posant $\varepsilon(x)=[\varepsilon_1(x)]^\lambda$, $\varepsilon_1(\alpha)t_s=v_1$, $t_r=u_1$, l'équation (30) devient

$$u_1^\lambda+v_1^\lambda=\mathrm{E}_1(\alpha)(1-\alpha)^{(m-1)\lambda}w_1^\lambda. \tag{31}$$

Voilà une équation qui ne diffère de l'équation (19) dont elle dérive qu'en ce que le nombre m est diminué d'une unité. Donc, si on lui applique la même méthode, on obtient, à partir d'elle, une équation de même forme où m a deux unités de moins que dans (19).

Par répétition de ce procédé, on arrive à une équation de même forme où $m=1$. Mais, pour celle-ci, la méthode qui suppose $m>1$ n'est plus applicable. On obtient donc une équation de la forme

$$u^\lambda+v^\lambda=\mathrm{E}(x)(1-x)^\lambda w^\lambda. \tag{32}$$

L'impossibilité de cette équation se démontre facilement, car on démontre ce qui suit : la forme $u^\lambda+v^\lambda$, si elle contient le facteur $1-x$, doit le contenir au moins $\lambda+1$ fois.

Pour le démontrer, je pose de nouveau

$$u=a+(1-x)^2\mathrm{P}, \qquad v=b+(1-\alpha)^2\mathrm{Q}.$$

On a, de nouveau,

$$u+\alpha^r v\equiv a+b-rb(1-x) \qquad [\text{mod. } (1-x)^2]. \tag{33}$$

Mais comme $u^\lambda+v^\lambda$ est divisible par $1-\alpha$, et, par suite, également, au moins un des facteurs de cette expression, qui ont tous la forme $u+x^r v$, il s'ensuit que $a+b$ doit être divisible par $1-x$, et, par suite, également par λ.

La congruence (33) se change donc en

$$u+\alpha^r v\equiv -rb(1-\alpha), \qquad \text{mod. } (1-x)^2. \tag{34}$$

Pour $r=0$, en particulier,

$$u+v\equiv 0, \qquad \text{mod. } (1-x)^2. \tag{35}$$

Tous les facteurs de la forme $u^\lambda+v^\lambda$ sont donc divisibles par $1-x$; mais le facteur $u+v$ est divisible par $(1-\alpha)^2$. Le nombre de tous les facteurs $1-x$ contenus dans $u^\lambda+v^\lambda$ est donc au moins $\lambda+1$; ce qu'il fallait démontrer.

L'équation (32), dans laquelle w n'est pas divisible par $1-x$, contient donc en elle la contradiction que la partie gauche est divisible par $(1-x)^{\lambda+1}$, et la partie de droite ne l'est pas. Cette équation est donc impossible, et, par suite, également l'équation (19) dont elle dérive, c'est-à-dire qu'une équation semblable ne peut être satisfaite par des nombres entiers complexes.

L'équation $u^\lambda + v^\lambda + w^\lambda = 0$ est donc, dans les deux cas, impossible.

§ V. — Démonstration d'un théorème de Kummer,

par Léopold Kronecker (1856).

Dans son mémoire sur la théorie des N. C., composés des racines $\lambda^{\text{ièmes}}$ de l'unité et de nombres entiers (*Crelle*, t. XX, p. 130, 1850), M. Kummer a donné ce théorème important : *La condition nécessaire et suffisante pour que le premier facteur du nombre de classes* H *soit divisible par* λ *consiste en ce qu'un quelconque des* $\frac{\lambda-3}{2}$ *premiers nombres bernoulliens soit divisible par* λ.

On peut démontrer ce théorème d'une manière très simple.

En effet, si on conserve les notations de M. Kummer, tout se réduit à examiner si la congruence

$$\psi(\gamma^{2n-1}) = b_0 + b_1\gamma^{2n-1} + \ldots + b_{\lambda-2}\gamma^{(\lambda-2)(2n-1)} \equiv 0 \pmod{\lambda}$$

est ou n'est pas satisfaite pour une quelconque des valeurs de $n = 1, 2, \ldots \mu$.

Donc, puisqu'on a (p. 474) $\lambda b_k = \gamma\gamma_{k-1} - \gamma_k$, il s'agit d'examiner la congruence

$$\text{(I)}\quad \lambda\psi(\gamma^{2n-1}) = \Sigma(\gamma\gamma_{k-1} - \gamma_k)\gamma^{(2n-1)k} \equiv 0 \pmod{\lambda^2},$$

où le signe Σ s'étend à toutes les valeurs de

$$k = 0, 1, 2 \ldots (\lambda - 2).$$

Partons de l'identité $\gamma^k - (\gamma^k - \gamma_k) = \gamma_k$. En l'élevant à la

puissance $2n$ et en observant que le nombre entier $\gamma^k - \gamma_k$ est un multiple de λ, on obtient la congruence

$$\gamma^{2nk} - 2n\gamma^{(2n-1)k}(\gamma^k - \gamma_k) \equiv \gamma_k^{2n} \pmod{\lambda^2}.$$

En remplaçant k par $k-1$ et en multipliant par γ^{2n-1}, il vient

$$(1-2n)\gamma^{2nk} + 2n\gamma_{k-1}\gamma^{(2n-1)k+1} \equiv \gamma^{2n}\gamma_{k-1}^{2n} \pmod{\lambda^2}.$$

La première s'écrit d'ailleurs ainsi

$$(1-2n)\gamma^{2nk} + 2n\gamma_k\gamma^{(2n-1)k} \equiv \gamma_k^{2n} \qquad \pmod{\lambda^2}.$$

En retranchant cette congruence de la précédente, on obtient

$$2n(\gamma\gamma_{k-1} - \gamma_k)\gamma^{(2n-1)k} \equiv \gamma^{2n}\gamma_{k-1}^{2n} - \gamma_k^{2n} \qquad \pmod{\lambda^2}.$$

Donc, on aura de même

$$2n\Sigma(\gamma\gamma_{k-1} - \gamma_k)\gamma^{(2n-1)k} \equiv \gamma^{2n}\Sigma\gamma_{k-1}^{2n} - \Sigma\gamma_k^{2n} \pmod{\lambda^2}.$$

Or, comme les nombres $\gamma_0, \gamma_1 \dots \gamma_{\lambda-2}$ et les nombres $1, 2, \dots (\lambda-1)$ sont les mêmes à l'ordre près, on a enfin

$$\text{(II)}\quad 2n\Sigma(\gamma\gamma_{k-1} - \gamma_k)\gamma^{(2n-1)k}$$
$$\equiv (\gamma^{2n} - 1)[1^{2n} + 2^{2n} + \dots + (\lambda-1)^{2n}] \pmod{\lambda^2}.$$

Le nombre $2n$ est moindre que λ. On voit donc que la discussion de la congruence (I) se réduit à la question de savoir si le second membre de la congruence (II) est divisible par λ^2.

Cela n'a pas lieu pour la valeur $2n = 2\mu = \lambda - 1$. Car suivant l'hypothèse (faite par M. Kummer) que le nombre $\gamma^\mu + 1$ ne soit pas divisible par λ^2, le nombre $\gamma^{2\mu} - 1$ ne contiendra qu'une fois le facteur λ, et, en vertu du théorème de Fermat, la somme $1^{\lambda-1} + 2^{\lambda-1} + \dots + (\lambda-1)^{\lambda-1}$ sera congrue à -1 suivant le module λ.

Ensuite, pour décider si le produit

$$\gamma^{2n-1}[1^{2n} + 2^{2n} + \dots + (\lambda-1)^{2n}]$$

est divisible par λ^2 pour une des valeurs de

$$n = 1, 2, \dots (\mu - 1),$$

observons que, dans ce cas, le nombre $\gamma^{2n} - 1$ n'est pas divisible par λ et que l'expression connue de la somme $1^{2n} + 2^{2n} + \ldots + (x-1)^{2n}$ en fonction rationnelle, entière, de x fournit la congruence

$$1^{2n} + 2^{2n} + \ldots + (\lambda - 1)^{2n} \equiv B_n \lambda \pmod{\lambda^2},$$

B_n désignant le $n^{ième}$ nombre bernoullien.

Donc, pour que la congruence (I) ait lieu pour une quelconque des valeurs de $n = 1, 2, \ldots \mu$, il faut et il suffit que la congruence $B_n \equiv 0 \pmod{\lambda}$ soit satisfaite pour une quelconque des valeurs de $n = 1, 2, \ldots, \mu - 1$; ce qu'il fallait démontrer.

§ VI. — Sur les équations cubiques à coefficients rationnels,

par L. Kronecker (1859).

« Le théorème de Fermat contient dans le cas le plus simple la proposition que l'égalité $r^3 + s^3 - 1 = 0$ ne peut être satisfaite par des valeurs rationnelles de r et s, non nulles.

« Par la substitution

$$r = \frac{2a}{3b-1}, \qquad s = \frac{3b+1}{3b-1},$$

on obtient

$$(3b-1)^3(r^3 + s^3 - 1) = 2(4a^3 + 27b^2 + 1) ;$$

et il en découle que $4a^3 + 27b^2 + 1 = 0$ ne peut être satisfaite par des valeurs rationnelles de a, b que si $a = -1$, $b = \pm \frac{1}{3}$. Inversement, $r^3 + s^3 - 1 = 0$ serait une conséquence de la précédente égalité. »

Dans ce qui suit, l'auteur remarque que $4a^3 + 27b^2$ est, au signe près, le discriminant de $x^3 + ax + b = 0$, et il ne s'occupe plus que des racines de $x^3 - x \pm \frac{1}{3}$.

§ VII. — Table des valeurs des 62 premiers nombres de Bernoulli,

par le Professeur J. C. Adams, M. A. F. R. S. de Cambridge (*Journal de Crelle,* t. LXXXV, p. 269, 1878).

	NUMÉRATEUR	DÉNOMINATEUR	N^{os}
	1	6	1
	1	30	2
	1	42	3
	1	30	4
	5	66	5
	691	2730	6
	7	6	7
	3617	510	8
	43867	798	9
	1 74611	330	10
	8 54613	138	11
	2363 64091	2730	12
	85 53103	6	13
	2 37494 61029	870	14
	861 58412 76005	14322	15
Divisible par 37.	770 93210 41217	510	16
	257 76878 58367	6	17
	26315 27155 30534 77373	19 19190	18
	2 92999 39138 41599	6	19
	2 61082 61082 64491 22051	13530	20
	15 20097 64391 80708 02691	1806	21
Divisible par 59.	278 33269 57930 10242 35023	690	22
	5964 51111 59391 21632 77961	282	23
	560 94033 68997 81768 62491 27547	46410	24
	49 50572 05244 07964 82124 77525	60	25
	80116 57181 35489 95734 79249 91853	1590	26
	29 14996 36348 84862 42141 81238 12691	798	27
	2479 39292 93132 26753 68543 57396 63229	870	28
Divisible par 67.	84483 61334 88800 41862 14677 59940 36021	354	29
Le soixantième a 113 chiffres au numérateur et 10 au dénominateur.			

CHAPITRE X

DE KUMMER A MIRIMANOFF

§ I. — Extension du théorème de Fermat,

par A. GENOCCHI (1876).

L'auteur se propose de prouver que, x, y, z étant les racines de l'équation $v^3 - pv^2 + qv - r = 0$, à coefficients rationnels et entiers, l'équation $x^7 + y^7 + z^7 = 0$ est impossible.

Elle s'écrit, en posant $pq - r = l$, puis en remplaçant ql, l par p^2q, p^3l, $7l^2 - 7l(1 - q - q^2) + 1 = 0$.

Il faut donc que $(1 - q - q^2)^2 - \frac{4}{7}$ soit un carré ; posant $q - \frac{1}{2} = \frac{s}{t}$, irréductible, il faut que

$$\left(\frac{s^2 + 3t^2}{4}\right)^2 - \frac{4t^4}{7} = \left(\frac{u}{4}\right)^2.$$

On distingue ici plusieurs cas : s, t impairs ; t impair, p pair ; t pair, s impair.

1° s, t impairs ; u sera pair, $\frac{u}{4}$ impair, et il s'ensuivra, en posant $\frac{t}{7} = s't'$,

$$\frac{s^2 + 3t^2 + u}{4} = 2s'^4, \quad \frac{s^2 + 3t^2 - u}{4} = 2.7^3t'^4.$$

Les ajoutant, on aurait $\frac{s^2 + 3t^2}{4} = s'^4 + 7t'^4$, ce qui ne peut être, s', t', $\frac{s^2 + 3t^2}{4}$ étant impairs.

Méthodes analogues dans les autres cas, avec descente infinie dans le dernier.

§ II. $X^n + Y^n = Z^n$, par Liouville (1879).

Considérons $U = \int \frac{\alpha^{n-1} d\alpha}{(1-\alpha^n)^{\frac{1}{n}}}$, ainsi que trois polynomes X, Y, Z, fonctions algébriques, rationnelles et entières, de degré quelconque, en t.

Si l'on pose $\alpha = \frac{X}{Z}$, l'intégrale U s'exprime par

$$\int \frac{Z}{Y}\left(\frac{X}{Z}\right)^{n-1} d\left(\frac{X}{Z}\right).$$

Or, il est clair que l'expression primitive est celle d'une fonction rationnelle et entière de $\sqrt[n]{1-\alpha^n}$, c'est-à-dire de $\frac{Y}{Z}$. On en conclut que nul des facteurs de Y ne figure au dénominateur de la fraction $\frac{X^{n-1}}{YZ^n}\left(Z\frac{dX}{dt} - Y\frac{dZ}{dt}\right)$ qui n'est autre que $\frac{dU}{dt}$, en vertu des formules précédentes.

Comme X, Y, Z n'ont pas de facteur commun, il faut que $Z^2\frac{d\left(\frac{X}{Z}\right)}{dt}$ soit le produit de Y par une fonction A, algébrique et entière. Mais

$$Z^2\frac{d\left(\frac{X}{Z}\right)}{dt} = -Z^2\frac{Y^{n-1}}{X^{n-1}}\frac{d\left(\frac{Y}{Z}\right)}{dt}.$$

ou bien

$$A + \frac{Z^2Y^{n-2}}{X^{n-1}}\frac{d\left(\frac{Y}{Z}\right)}{dt} = 0.$$

Il en résulte que X^{n-1} divise $Z^2\frac{d\left(\frac{Y}{Z}\right)}{dt}$.

Soit B le quotient. Posons, pour abréger, $\frac{Y}{Z} = P$.
On doit avoir, en conséquence,

$$\frac{dP}{dt} = \frac{B}{Z^2} X^{n-1} = BZ^{n-3}(1 - P^n)^{\frac{n-1}{n}};$$

d'où

$$\frac{\frac{dP}{dt}}{(1 - P^n)^{\frac{n-1}{n}}} = BZ^{n-3}.$$

Dans cette identité, le premier membre devient infini si l'on y substitue les racines de $P^n - 1$; le second, étant une fonction entière, prend une valeur finie pour toute valeur déterminée de la variable. L'égalité est donc impossible.

Il est clair que le cas où $n = 1$ échappe à l'analyse précédente, ainsi qu'il devait être.

Pour un cas particulier, celui où $n = 2$, les résultats précédents étaient contenus dans un théorème général énoncé par Jacobi dans ses *Opuscules*.

§ III. $X^n + Y^n + Z^n = 0$,

par Korkine (1880).

Dans les C. R. du 29 décembre 1879, M. Liouville a donné une démonstration de l'impossibilité de l'équation

$$(1) \qquad X^n + Y^n + Z^n = 0,$$

par des polynomes X, Y, Z, que je modifie comme il suit :

Lorsqu'il est possible de satisfaire à l'équation (1) au moyen de trois fonctions entières de t, dont aucune ne se réduit à zéro, on peut toujours supposer que ces fonctions, prises deux à deux, n'ont pas de facteur commun.

Soit Z celui des trois, dont le degré m n'est pas inférieur aux degrés des autres. On voit facilement que le degré de l'un, au moins, des polynomes X, Y est égal à m. Soit X de degré $m - \lambda$, $\lambda \geqslant 0$.

En différentiant par rapport à t, on a, d'après

$$\left(\frac{Y}{X}\right)^n + \left(\frac{Z}{X}\right)^n + 1 = 0,$$

$$Y^{n-1}(XY' - YX') = Z^{n-1}(ZX' - XZ').$$

Il résulte de cette équation, Y, Z n'ayant pas de facteur commun, que les expressions $\frac{XY'-YX'}{Z^{n-1}}$, $\frac{ZX'-XZ'}{Y^{n-1}}$ sont égales à une fonction entière, ou, au moins, à une constante non nulle. Or, comme les degrés des numérateurs ne surpassent pas $2m - \lambda - 1$, ceux des dénominateurs étant $m(n-1)$, il suit que la différence $2m - \lambda - 1 - m(n-1)$ est nulle ou plus grande que zéro, c'est-à-dire qu'on a

$$m(3-n) \geqslant \lambda + 1,$$

et, par conséquent, $n < 3$.

Il se trouve ainsi démontré que le cas connu de résolubilité, celui de $n = 2$, est unique, si l'on fait abstraction du cas $n = 1$, où la solution est évidente.

§ IV. $a^n + b^n = c^n$,

par E. DE JONQUIÈRES (1884).

« Soit $a < b < c$; $c = a + i$, $i > 1$. Donc i divise b^n ; par suite, pour que b fût premier, il faudrait que i fût égal à b ou à une puissance de b. Or, il ne peut même pas être égal à b, car on aurait $a^n + b^n = (a+b)^n$.

« Ainsi, b^n est divisible par un entier i, plus petit que b. Donc la racine b ne peut pas être un nombre premier, et l'on a ces deux théorèmes :

I. *La somme des puissances $n^{\text{ièmes}}$ de deux nombres premiers n'est jamais égale à la puissance $n^{\text{ième}}$ d'un nombre entier.*

II. *Si $a^n + b^n = c^n$ est satisfaite, le nombre $b (b > a)$ est toujours composé, que a soit ou ne soit pas premier.*

« D'autre part, posons $c = b + j$. j est inférieur à a. Si

donc a est premier, j, divisant a^n, ne peut être que l'unité et l'on a ce théorème :

III. *Si* $a^n + b^n = c^n$ *est satisfaite et si* a *est premier, on a* $c - b = 1$. »

§ V. — Sur le théorème de Fermat,

par E. CATALAN (1886).

« En suivant la voie indiquée par M. de Jonquières, voici d'autres propositions : Je suppose a premier et inférieur à b.

I. $a - 1 =$ mult. n.

II. $a^n - 1 =$ mult. nb.

III. Tout diviseur premier de $c - a$ divise $a - 1$.

IV. $a + b$ et $c - a$ sont premiers entre eux.

V. $2a - 1$ et $2b + 1$ sont premiers entre eux.

VI. a est compris entre $\sqrt[n]{nb^{n-1}}$ et $\sqrt[n]{n(b+1)^{n-1}}$.

VII. a et b surpassent n.

VIII. c est compris entre $a + b$ et $\frac{a+b}{2}$.

IX. Aucun des nombres $a + b$, $c - a$, $c - b$ n'est premier. »

§ VI. — En connexion avec le théorème de Fermat,

par G. B. MATHEWS (1885-6).

« De $x^p \equiv x \pmod{p}$, on tire, si $x^p + y^p = z^p$, $z \equiv (x + y)$; d'où $(tp + x + y)^p = x^p + y^p$, ou $(x + y)^p - x^p - y^p \equiv 0 \pmod{p^2}$. Or, le premier membre est égal à $pxy(x + y)\varphi(x, y)$. Donc, on a $xy(x + y)\varphi \equiv 0 \pmod{p}$.

« Si on peut démontrer que la congruence $\varphi \equiv 0$ est insoluble, x, y ou z devra être divisible par p. »

L'auteur suppose successivement $p = 3, 5, 7, 11, 13, 17$ et établit l'insolubilité, excepté pour 7 et 13. Exemple : $p = 5$; $4\varphi = (2x + y)^2 + 3y^2$. « Or, -3 est un non-résidu de 5. Donc, la congruence n'admet que la solution $y \equiv 0$, $2x + y \equiv 0$, c'est-à-dire $y \equiv 0$, $x \equiv 0$; inacceptable, x, y étant premiers relatifs. Exemple : $p = 7$; $\varphi = (x^2 + xy + y^2)^2$. — 3 étant

un résidu de 7, la congruence admet $x \equiv 2$, $y \equiv 1$ et $x \equiv 4$, $y \equiv 1$. »

§ VII. — **Note sur le théorème de Fermat,**

par l'ingénieur P. Borletti (1887).

« Si z est premier, $x^n + y^n = z^n$ n'a pas de solution.

« On a $(x+y)(x^{n-1} - yx^{n-2} + \ldots + y^{n-1}) = z^n$ par hypothèse. Or z est supposé premier ; on en déduit $x+y = z^\alpha$, $x^{n-1} + \ldots + y^{n-1} = z^\beta$.

« Je dis que $\alpha < \beta$. En effet, si on pose $y = x - q$, la seconde équation devient

$$x^{n-2}q + x^{n-4}y^2q + x^{n-6}y^4q + \ldots + xy^{n-3}q + y^{n-1} = z^\beta,$$

et, comme

$$x < x^{n-2}q + \ldots + xy^{n-1}q \quad \text{et} \quad y < y^{n-1},$$

on en déduit $\quad x+y < z^\beta, \quad$ d'où $\quad \alpha < \beta$.

« Cela posé, la seconde équation peut s'écrire, en y remplaçant y par $z^\alpha - x$, $nx^{n-1} + Az^\alpha = z^\beta$; ce qui montre que nx^{n-1} doit être divisible par z^α, et, x, z étant premiers relatifs, on doit avoir $n = kz^\alpha$; d'où, puisque n est premier, $k = 1$, $\alpha = 1$, $n = z$.

« Considérons maintenant l'équation $x^n + y^n = n^n$.

« Elle se décompose ainsi :

$$x + y = n, \quad x^{n-1} - yx^{n-2} + \ldots + y^{n-1} = n^{n-1},$$

et, comme on ne peut avoir $x^n + y^n = (x+y)^n$, l'équation $x^n + y^n = n^n$ est impossible et, par suite, aussi l'équation $x^n + y^n = z^n$. »

En réalité, $x+y$ est divisible par n^{n-1}.

§ VIII. — **Sur l'équation** $x^{37} + y^{37} = z^{37}$,

par D. Mirimanoff, de Genève (1893).

« Soit $x^{37} + y^{37} = z^{37}$. Je suppose que x, y, z fassent partie du domaine d'intégrité $(\theta + \theta^{-1})$, θ étant une racine primitive

de $x^{37} - 1 = 0$, et que z, premier à x, y, soit divisible par $\beta = (1 - \theta)(1 - \theta^{-1})$.

« L'équation rentre dans la classe des équations

$$x^{37} + y^{37} = \varepsilon\beta^{X} z^{37},$$

ε étant une unité quelconque du domaine $(\theta + \theta^{-1})$, X un multiple de 37.

« Je supposerai de plus que les nombres $(x + y)^2$ et xy fassent partie du domaine $(\theta + \theta^{-1} + \theta^{g} + \theta^{-g})$, g étant une racine primitive pour le module 37.

$$x^{37} + y^{37} = (x + y)\prod_{i=1}^{i=18}(x^2 + y^2 + \delta xy),$$

δ étant la période $\theta + \theta^{-1}$.

« Le second facteur du nombre de classes n'étant pas divisible par 37, il vient

$$x + y = e_0\beta^{X-18}u_0^{37}\ (1), \qquad (x + y)^2 - (2 - \delta)xy = e_i\beta u_i^{37},$$

e_0, e_i étant des unités complexes ; u_0, u_i des nombres existants, premiers à β^{X}.

« On a, pour $i = 1$, $(x + y)^2 - \beta xy = e_1\beta u_1^{37}$, puisque

$$2 - \delta = \beta.$$

« Posons $\frac{1}{e_1} = e$, $e_1 u_1 = v_1$. Il viendra

$$(x + y)^2 - \beta xy = e^{36}\beta v_1^{37}.$$

« Or, l'unité e^{36} peut être remplacée par le produit $\varepsilon_{18}^{6}\varepsilon_{9}^{6}\varepsilon_{6}^{2}\varepsilon_{3}^{2}\varepsilon_{2}$, ces $\varepsilon_{18} \ldots \varepsilon_{2}$ étant des unités appartenant aux diviseurs de 18 ; parmi ces unités, deux seulement font partie du domaine

$$(\theta + \theta^{-1} + \theta^{g} + \theta^{-g}) ;$$

ce sont ε_0 et ε_3.

« Je pose $x = \varepsilon_9^3\varepsilon_3 x'$, $y = \varepsilon_0^3\varepsilon_3 y'$, $z = \varepsilon_9^3\varepsilon_3 z'$, $\dfrac{\varepsilon^{36}}{\varepsilon_9^6\varepsilon_3^2} = \mathrm{E}(\theta)$.

La dernière équation devient $(x' + y')^2 - \beta x'y' = \mathrm{E}(\theta)\beta v_1^{37}$.

« Or $x'y'$ étant invariable par la substitution P_9, qui a pour effet de remplacer θ par θ^{g^9}, il viendra, n entier,

$$- x'y' = \mathrm{E}(\theta^{g^9})n ;$$

par conséquent, $\frac{E(\theta)}{E(\theta^{9^0})} \equiv 1 \pmod{37}$.

« Les unités $\frac{E(\theta)}{E(\theta^{9^0})}$, $E(\theta)$, $E(\theta^{9^0})$ sont donc des puissances 37^{ièmes}.

« Posons $E(\theta)^{\frac{1}{37}} v_1 = \xi$; l'équation précédente devient

$$(x' + y')^2 - \beta x'y' = \beta\xi^{37}.$$

« J'applique à cette équation la substitution P_9 ; il viendra, en désignant par β'', ξ'' les conjugués de β, ξ,

$$(x' + y')^2 - \beta'' x'y' = \beta''\xi''^{37}.$$

« Si l'on tient compte de l'équation (1), on obtient, en posant $u'_0 = \zeta$, $\xi'' = \eta$, l'équation $\xi^{37} + \eta^{37} = \varepsilon_0 \frac{\beta'' - \beta}{\beta''} \beta^{-37}\zeta'^{37}$, ε_0 étant une unité complexe du domaine $(\theta + \theta^{-1})$.

« Cette équation rentre dans la classe des équations

$$x^{37} + y^{37} = \varepsilon\beta^{\chi} z^{37}$$

et les nombres $(\xi + \eta)^2$, $\xi\eta$ appartiennent de même que $(x + y)^2$ et xy au domaine $(\theta + \theta^{-1} + \theta^{9^0} + \theta^{-9^0})$.

« Voici comment on pourrait prouver que cette « descente » conduit à une conclusion impossible. »

L'auteur prouve que le module de la norme des ζ est plus petit que celui de la norme des z.

L'auteur suppose, en second lieu, qu'aucun des x, y, z n'est divisible par $1 - \theta$, et il conclut comme précédemment.

§ IX. $x^n + y^n = z^n$, par M. G. Korneck (1895).

« *Lemme*. — Soient les deux nombres n, impair, et k, premiers relatifs et non divisibles par un carré. Si l'on a, en nombres entiers, $nx^2 + ky^2 = z^n$, x sera divisible par n. »

Le rapporteur signale ces exemples du résultat contraire :

$n = 3$, $k = 1$, $x = y = z = 4$;

$n = 5$, $k = 3$, $x = 1$, $y = 3$, $z = 2$;

$n = 7$, $k = 65$, $x = 3$, $y = 1$, $z = 2$.

§ X. — Deuxième note en connexion avec le théorème de Fermat,

par G. Mathews (1895).

« Soit k entier, et $r = e^{\frac{2\pi i}{k}}$. Le produit $P_k = (r\Pi^\alpha + r^\beta + r^\gamma)$, étendu à toutes les trinités distinctes $r^\alpha, r^\beta, r^\gamma$ des racines de $x^k - 1 = 0$, s'annule si k est multiple de 3 et est entier dans les autres cas, égal à $\pm u_k^k$, u entier.

« Ainsi $P_7 = -2^7$, de sorte que $u_7 = -2$. »

L'auteur étudie les congruences $u_k \equiv 0$ (mod. $nk + 1$).

« Si on peut montrer que, lorsque n est donné, il y a une infinité de nombres premiers, $nk+1$, pour lesquels la congruence précédente n'est pas satisfaite, on aura démontré l'impossibilité de l'équation $x^n + y^n + z^n = 0$. »

§ XI. — Sur l'équation indéterminée $ax^{\lambda^t} + by^{\lambda^t} = cz^{\lambda^t}$,

par Edmond Maillet, Ingénieur des Ponts et Chaussées (1897).

On suppose a, b, c premiers à λ ; λ, premier impair ; et l'équation satisfaite.

Lemme. — *Si* $A \equiv A_0$ (mod. λ), *on a* $A^{\lambda^t} \equiv A_0^{\lambda^t}$ (mod. λ^{t+1}).

Démonstration facile, exposée par l'auteur. Le lemme est de Kummer.

Si donc x_0, y_0, z_0 sont les résidus de x, y, z divisés par λ, on aura $ax_0^{\lambda^t} + by_0^{\lambda^t} \equiv cz_0^{\lambda^t}$ (mod. λ^{t+1}).

Or, on a $x_0^{\lambda^t} \equiv (x_0^{\lambda^{t-1}})^\lambda \equiv x_0^{\lambda^{t-1}}$ (mod. λ).

Continuant ainsi, on arrive à $x_0^{\lambda^t} \equiv x_0$ (mod. λ), d'où $ax_0 + by_0 - cz_0 \equiv 0$ (mod. λ) et, en posant $a \equiv c\alpha$, $b \equiv c\beta$ (mod. λ), $c(\alpha x_0 + \beta y_0 - z_0) \equiv 0$ (mod. λ) ; $\alpha, \beta < \lambda$; ou $z_0 \equiv \alpha x_0 + \beta y_0$ (mod. λ).

Appliquant le lemme, on a $z_0^{\lambda^t} \equiv (\alpha x_0 + \beta y_0)^{\lambda^t}$ (mod. λ^{t+1}) ; d'où $ax_0^{\lambda^t} + by^{\lambda^t} \equiv c(\alpha x_0 + \beta y_0)^{\lambda^t}$ (mod. λ^{t+1}).

Soit maintenant $x_0 t_0 \equiv 1$, $y_0 t_0 \equiv r$ (mod. λ).

Appliquant encore le lemme, on a

$$(x_0 t_0)^{\lambda^t} \equiv 1, \qquad (y_0 t_0)^{\lambda^t} \equiv r^\lambda \pmod{\lambda^{t+1}}.$$

Multipliant par $t_0^{\lambda^t}$ la congruence antéprécédente, celle-ci devient $a + br^{\lambda^t} \equiv c(\alpha + \beta r)^{\lambda^t} \not\equiv 0 \pmod{\lambda^{t+1}}$, d'où ce théorème.

Théorème. — Pour que l'équation admette une solution, il faut que la dernière congruence en admette une en $\eta_0 (0 < \eta_0 < \lambda)$ et telle que $\alpha + \beta\eta_0 \not\equiv 0 \pmod{\lambda}$.

Application à l'équation $ax^{197} + by^{197} = cz^{197}$. — On suppose $a \equiv b \equiv c \equiv 1 \pmod{197}$.

« Legendre n'a pas démontré son impossibilité, même dans le cas $a = b = c = 1$. Il suffit, pour la démontrer, de prouver que la dernière congruence, qui s'écrit $1 + r^{197} \equiv (1 + r)^{197} \pmod{197^2}$ n'a pas de solution.

« Pour cela, on formera les résidus $\pmod{197^2}$ des puissances $197^{\text{ièmes}}$ des $\frac{197 - 1}{2}$ ou 98 premiers nombres. »

Dans le tableau de ces résidus, établi par l'auteur, on ne peut trouver un nombre r vérifiant la congruence ci-dessus. L'impossibilité de l'équation proposée est donc démontrée.

« Prenons encore $\lambda = 199$, $\lambda = 211$, les seuls nombres premiers < 223. On reconnaît l'existence des nombres premiers $797 = 4.199 + 1$, $2111 = 10.211 + 1$. Donc, d'après les théorèmes de Sophie Germain et de Legendre, l'équation est impossible dans ces deux cas. »

§ XII. — Memoria bibliografica sull' ultimo teorema di Fermat,

par Dionisio Gambioni (1901).

I. L'auteur reprend les théorèmes de de Jonquières et en ajoute d'autres : x et z sont-ils composés comme l'est y ?

II. Il démontre l'impossibilité de $x^4 - y^4 = z^2$.

« Si elle est possible, on peut grouper toutes les solutions dont le produit xyz a la même valeur ; il est évident que

parmi ces produits il y en a un plus petit que les autres sans être nul.

« Supposons que la solution considérée appartienne à ce groupe et démontrons qu'on peut toujours en obtenir une autre formée de trois nombres dont le produit est plus petit que le produit minimum xyz. Cette conséquence serait absurde ; donc, l'équation proposée est impossible.

« Une seule des trois indéterminées est paire. Ce n'est pas x ; car, si c'était x, x^4 serait $4m$, et on aurait

$$4m = (4k + 1) + (4k' + 1),$$

c'est-à-dire $$2m = 2m' + 1.$$

« 1° $y = 2m$. Posons $y = 2\alpha\beta$, d'où $x^2 \pm z = 2\alpha^4, x^2 \mp z = 8\beta^4$, et, par suite, $x^2 = \alpha^4 + 4\beta^4$, c'est-à-dire

$$(x + \alpha^2)(x - \alpha^2) = 4\beta^4.$$

« Posons maintenant $\beta = \delta\gamma$; nous avons

$$x + \alpha^2 = 2\delta^4, \qquad x - \alpha^2 = 2\gamma^4 ;$$

d'où $$\delta^4 - \gamma^4 = \alpha^2.$$

« On a donc une seconde solution, pour laquelle le produit $\alpha\delta\gamma$ est non seulement plus petit que xyz, mais encore que y.

« 2° $y = 2m + 1$. C'est z qui est pair. Posons $z = 2\alpha\beta$. On a

$$x^2 + y^2 = 2\alpha^2, \qquad x^2 - y^2 = 2\beta^2,$$

d'où $x^2 = \alpha^2 + \beta^2, \quad y^2 = \alpha^2 - \beta^2, \quad (xy)^2 = \alpha^4 - \beta^4$;

xy, α, β est donc une solution et le produit $(xy)\alpha\beta = \frac{xyz}{2}$.

« On en conclut que l'équation proposée n'a pas de solution.

$$x^4 + y^4 = z^4.$$

« On l'écrit $z^4 - y^4 = (x^2)^2$; impossible d'après ce qui précède.

« On l'écrit autrement $(x^2)^2 + (y^2)^2 = (z^2)^2$, vérifiée par

$$x^2 = p^2 - q^2, \qquad y^2 = 2pq, \qquad z^2 = p^2 + q^2,$$

d'où l'on tire $(xz)^2 = p^4 - q^4$, démontrée impossible. Cela montre que $x^2 + y^2 = z^2$ n'est pas soluble en trois carrés.

« *Corollaire*. — L'équation $x^{2^n}+y^{2^n}=z^{2^n}$ est impossible, car elle s'écrit $(x^{2^{n-2}})^4+(y^{2^{n-2}})^4=(z^{2^{n-2}})^4$. »

$$x^2+y^2=z^2.$$

L'auteur démontre que 3 et 4 sont des diviseurs de x ou de y, et que 5 divise x ou y ou z, de sorte que xyz est divisible par 60.

III. $$x^5+y^5+z^5=0.$$

« Dans cette note, je me propose de donner une démonstration simple et brève de l'impossibilité de cette équation. » Il part de $x=p+q$, $y=p-q$, d'où

$$2p[p^4+5q^2(q^2+2p^2)]+z^5=0,$$

et, sans l'expliquer, il pose $a^2=q^2+2p^2$, ce qui lui permet d'écrire $2p[(p^2)^2+5(qa)^2]+z^5=0$.

§ XIII. — Mémoire de L. Calzolari ; essai pour démontrer le théorème de Fermat,

FERRARE (1855).

I. $$x^3+y^3=z^3. \qquad (1)$$

« Soit $z=x+u=y+v$, d'où

$$z^2-x^2-y^2+\frac{ux^2+vy^2}{z}=0.$$

Si (1) est possible, en posant $\frac{ux^2+vy^2}{z}=w_1$, w_1 doit être entier. L'équation peut s'écrire

$$z-x-y+\frac{ux+vy+w_1}{z}=0.$$

ou $z=x+y-w$, et w doit être entier.

« On en tire

$$x=v+w, \qquad y=u+w, \qquad z=u+v+w,$$
$$z^3-3(u+v)z^2+3(u^2+v^2)z-(u^3+v^3)\equiv 0.$$

« Donc $\frac{u^3+v^3}{z}$, c'est-à-dire $\frac{u^3+v^3}{u+v+w}$ doit être entier.

« Opérant avec x, y, on verrait de même que

$$\frac{(u-v)^3-u^3}{v+w}, \qquad \frac{(v-u)^3-v^3}{u+w}$$

doivent être entiers. »

Ces trois fractions s'écrivent

$$\frac{(u+v)(u+v+\sqrt{3uv})(u+v-\sqrt{3uv})}{u+v+w},$$

$$\frac{v(v+\sqrt{3u(v-u)})(v-\sqrt{3u(v-u)})}{v+w},$$

$$\frac{u(u+\sqrt{3v(u-v)})(u-\sqrt{3v(u-v)})}{u+w},$$

et l'auteur conclut : « excluant les valeurs nulles et négatives, la seule valeur de w qui puisse rendre entière la première expression est $\sqrt{3uv}$, pourvu que $3uv$ soit un carré, et, chacune des autres est $\sqrt{3u(v-u)}$, $\sqrt{3v(u-v)}$; ce qui exigerait que $u=v=0$. Donc, l'équation (1) est impossible. »

Calzolari applique ce procédé à $x^2+y^2=z^2$; et trouve pour z, x, y les valeurs

$$\frac{(u+v+\sqrt{2uv})(u+v-\sqrt{2uv})}{u+v+w},$$

$$-\frac{(v+\sqrt{2uv})(v-\sqrt{2uv})}{v+w}, \qquad -\frac{(u+\sqrt{2uv})(u-\sqrt{2uv})}{u+w};$$

il pose $w=\sqrt{2uv}$; d'où

$$z=u+v-\sqrt{2uv}, \quad x=-v+\sqrt{2uv}, \quad y=-u+\sqrt{2uv},$$

avec la condition que $2uv$ soit un carré.

II. $$x^n+y^n=z^n. \qquad (2)$$

Procédant comme précédemment, l'auteur réduit les expressions de la forme $z^{n-1}-x^{n-1}-y^{n-1}+w_{n-1}$ à l'expression $z-x-y+w$.

Comme précédemment, il prouve que, si l'équation (2) est vérifiée,

$$\frac{u^n + v^n}{z}, \qquad \frac{u^n - (u - v)^n}{x}, \qquad \frac{v^n - (v - u)^n}{y}$$

doivent être entiers.

Il reste à chercher les valeurs que doit prendre w pour qu'il en soit ainsi.

« D'abord $\frac{u^n + v^n}{u + v + w}$. On a (théorème de Côtes)

$$u^n + v^n = (u + v)\left[u^2 - 2uv\cos\frac{\pi}{n} + v^2\right]$$
$$\left[u^2 - 2uv\cos\frac{3\pi}{n} + v^2\right] \ldots \left[u^2 - 2uv\cos\frac{n-2}{n} + v^2\right].$$

Or, $u^2 - 2uv\cos\frac{\lambda\pi}{n} + v^2$

$$= \left(u + v + 2\sqrt{uv}\cos\frac{\lambda\pi}{2n}\right)\left(u + v - 2\sqrt{uv}\cos\frac{\lambda\pi}{2n}\right).$$

Donc w sera entier si $2\sqrt{uv}\cos\frac{\lambda\pi}{2n}$ est entier.

Avec les deux autres expressions, on trouve que

$$2\sqrt{u(v - u)}\cos\frac{\lambda'\pi}{2n} \qquad \text{et} \qquad 2\sqrt{v(u - v)}\cos\frac{\lambda''\pi}{2n}$$

doivent être entiers.

Ces deux dernières conditions sont évidemment incompatibles, une expression seule étant réelle, et elles le sont aussi avec la première, la première expression étant seule symétrique en u, v. L'équation (2) est donc impossible. »

§ XIV. — **Prétendues démonstrations du théorème de Fermat** (1909-10).

Voici des extraits des rapports de Fleck, de Perron, et Mannenchen.

« L'auteur confond les divisibilités algébrique et arithmétique. Ainsi, par exemple, $z^2 + zx + x^2$, n'étant pas divisible

par des facteurs linéaires réels, ne pourrait avoir aucun facteur commun avec $z - x$. Cependant pour $z = 10$, $x = 1$, on a $z^2 + zx + x^2 = 3.37$, $z - x = 9$. »

« L'auteur veut démontrer que les égalités

$$(a+2)^n - (a+1)^n = a^n,$$
$$(a+2)^n - (a+1)^n = x^n, \qquad (a+2)^n - y^n = z^n$$

sont insolubles rationnellement. Il démontre exactement que la première est insoluble en nombres entiers ; tout le reste est confus. »

« $t^n = a^n - (a - x)^n$. Comme, à gauche, il y a une puissance $n^{\text{ième}}$, la partie de droite doit se composer de n facteurs égaux ; et, en deux pages, tout est démontré. »

« L'auteur soutient que, parce qu'une grandeur peut être représentée par une fraction continue indéfinie périodique, cette grandeur doit être irrationnelle.

« Cela est faux ; car il est bien connu que la fraction continue indéfinie $a + \cfrac{b}{a + \cfrac{b}{a + \dots}}$ a la valeur $\frac{a + \sqrt{a^2 + 4b}}{2}$, de laquelle on peut trouver beaucoup de valeurs rationnelles, par exemple, pour $a = b - 1$, la valeur b. » Rapporteur : A. Fleck (Berlin).

« L'auteur explique que l'on peut également démontrer le théorème pour les sinus et les cosinus, et, pour que l'humour ne manque pas, il continue ainsi : « *cujus rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet* ». Rapporteur : O. Perron (Munich).

« L'auteur, B. Lindt, donne un aperçu, incomplet, il est vrai, mais de valeur réelle, sur l'histoire du Problème et les essais de résolution autant qu'ils emploient les moyens élémentaires.

« L'auteur cite certaines inégalités : $y - x > 2^n - 1$ est exacte ; mais la démonstration est fausse. z est compris entre x et $x\frac{n}{n-1}$, entre y et $y\frac{n}{n-1}$; celle-ci seule est

exacte. Suit l'inégalité $y < z < y\frac{n+1}{n}\cdot$ De celle, donnée par moi plus haut, $x^n > ny^{n-1}(z-y)$, si on remarque que

$$x < y, \qquad x > n(z-y),$$

alors suit $y > n(z-y)$, ou $z < y\frac{n+1}{n}\cdot$ Si une pareille inégalité vaut pour x et z, je n'ai encore pu le démontrer solidement.

« L'appendice apporterait la plus grande aide, s'il était exact. Là se place cette proposition : l'équation de Fermat est impossible en nombres entiers x, y, z, premiers avec n. Dans le cas $n = 6m - 1$, l'un d'eux doit être divisible par $3n^2$. » Rapporteur : A. Fleck.

§ XV. $x^l + y^l + z^l = 0$ et le critérium de Kummer, par D. Mirimanoff (1905).

« Nous appellerons critérium de Kummer la proposition suivante qu'il a établie (*Abh.*, 1857) : Si cette équation admet la solution α, β, γ, nombres premiers à l, chacun des six couples α, β ; β, α ; α, γ . . . vérifie les $\frac{l-3}{2}$ congruences $B_{\frac{l-i}{2}}P_i(x, y) \equiv 0$ (mod. l), où $i = 3, 5, 7, \ldots (l-2)$. $\frac{P_i}{(x+y)^i}$ étant, pour $v = 0$, la dérivée $i^{ème}$ de $\log(x + e^v y)$ par rapport à v.

« On peut donner une autre forme à ce résultat. Appelons r le rapport de deux nombres α, β, γ (mod. l). Soit, d'autre part, $\frac{y}{x} = t$.

« Les congruences, avec $P(1, t)$, sont vérifiées par r.

« Les six valeurs de r sont distinctes en général ; le groupe est dit complet. S'il se réduit à trois ou à deux valeurs distinctes, il est dit incomplet.

« On remarque que $P_i(1, t)$ est divisible par $t(1-t)$. »

Cela posé, l'auteur calcule les neuf premiers polynomes P.

« Posant $\frac{l-1}{2}=v$, $i=2x+1$, les congruences, pour $x=1, 2, 3, 4$, pour $i=3, 5, 7, 9$ s'expriment par $B_{\frac{l-3}{2}}$, $B_{\frac{l-5}{2}}$, $B_{\frac{l-7}{2}}$, $B_{\frac{l-9}{2}}$.

« Supposons que l'un au moins de ces quatre nombres de Bernoulli ne soit pas divisible par l; l'une au moins des congruences admettra le groupe des racines r, correspondant à la solution α, β, γ.

« Premier cas: groupe complet. — Je dis qu'aucune des quatre congruences ne saurait admettre les racines r. En effet, $P(t)$ devant admettre six racines, sans compter zéro et un, est au moins du 8e degré. Nous n'avons donc à nous occuper que de P_9.

« Or $\frac{P_9}{t(1-t)}=1-246t+4047t^2-11572t^3+\cdots+t^6$, et, d'autre part, tout polynome admettant les six racines d'un groupe complet a la forme $1+3t+at^2+(2a-5)t^3+\cdots+t^6$. On devrait donc avoir $-246\equiv 3 \pmod{l}$, d'où $l=3$ ou $l=83$. Mais l'indice i doit être inférieur à l. Donc $l=83$.

D'autre part, on devrait avoir $-11572\equiv 2.4047-5$ (mod. 83), ce qui n'est pas. »

L'auteur traite de même les cas des groupes incomplets: $1, -2, -\frac{1}{2}$ et t^2+t+1, ce qui lui permet d'énoncer ce théorème: *L'équation $x^l+y^l+z^l=0$ est impossible en nombres entiers premiers à l si l'un au moins des nombres $B_{\frac{l-3}{2}}$, ... $B_{\frac{l-9}{2}}$ n'est pas divisible par l.*

« On pourrait de même examiner les congruences $P_{11}(t)\equiv 0$, $P_{13}(t)\equiv 0$, etc. On obtiendrait ainsi des conditions de plus en plus larges, mais ce n'est assurément pas ce moyen qui étendrait la démonstration à tous les l.

« Le théorème précédent comprend comme cas particuliers ceux de Kummer (*Abh.*, 1857) et ceux de Cauchy (*C. R.*, 1847, p. 181). »

L'auteur ajoute : « L'équation est impossible pour $l = 223$, 227, 229 (Cauchy) et pour tous les $l < 257$ (Legendre et Maillet). »

§ XVI. — Démonstration de deux des formules d'Abel, par P. Stackel (1903).

L'auteur part de la congruence

$$\frac{y^n + z^n}{y + z} \equiv (-1)^{\frac{n-1}{2}} n(yz)^{\frac{n-1}{2}}, \quad \text{mod. } (y + z)^2,$$

qui devient, si on admet $x^n + y^n + z^n = 0$,

$$\frac{x^n}{y + z} \equiv (-1)^{\frac{n+1}{2}} n(yz)^{\frac{n-1}{2}}.$$

y, z étant supposés premiers relatifs, $y + z$ et yz le sont aussi.

Soit p un facteur premier de $y + z$, contenu k fois ; il entrera α fois par exemple dans x ; d'où $k \leqslant \alpha n$.

Si $k < \alpha n$, $\frac{x^n}{y+z}$ contient encore p, et, par suite, $n(yz)^{\frac{n-1}{2}}$ le contient aussi.

Mais yz ne le contient pas ; donc n est divisible par p, d'où $p = n$. Par suite, l'hypothèse $k < \alpha n$ ne peut être admise que si $y + z$ est divisible par n. Alors $\frac{x^n}{y+z}$ est divisible par n seulement et $k = \alpha n - 1$.

Il suit de là que, pour $p \neq n$, nécessairement $k = \alpha n$, et que les deux seules possibilités suivantes sont à considérer : 1° $y + z$ n'est pas divisible par n ; alors on peut écrire $y + z = u^n$, u entier, d'où $x = u . u'$, u et u' premiers relatifs. 2° $y + z$ est divisible par n ; alors on peut poser $y + z = n^{n-1}u^n$, d'où $x = nu . u'$, nu et u' premiers relatifs.

Autant avec $z + x$, $x + y$. Et, comme un seul des trois peut être divisible par n, on aura, ou $y + z = u^n$, $z + x = v^n$, $x + y = w^n$, ou $y + z = n^{n-1}u^n$, $z + x = v^n$, $x + y = w^n$; d'où les formules d'Abel

$$2x = -u^n + v^n + w^n, \quad 2y = u^n - v^n + w^n, \quad 2z = u^n + v^n - w^n$$

ou $2x = -n^{n-1}u^n + v^n + w^n$, $2y = n^{n-1}u^n - v^n + w^n$,

$$2z = n^{n-1}u^n + v^n - w^n.$$

§ XVII. — Sur l'équation $x^3y + y^3z + z^3x = 0$ et $x^7 + y^7 + z^7 = 0$, par Hurwitz (1908).

La première équation est insoluble en nombres entiers. Supposons, en effet, que x, y, z soit une solution entière. Soient $u = (y, z)$, $v = (z, x)$, $w = (x, y)$, les p. g. c. d. de ces nombres pris deux à deux. Comme w, v sont premiers relatifs, x, divisible par chacun d'eux, l'est par leur produit ; de même, pour y et z. L'équation peut donc s'écrire

$$v^2w^3x'^3y' + w^2u^3y'^3z' + u^2v^3z'^3x' = 0.$$

Le premier terme est divisible par u^2, et comme u ne divise pas v, w, x', il divise y'.

Le dernier terme est divisible par y', et, comme y' ne divise pas v, z', x', il divise u^2.

Ainsi, chacun des nombres y' et u^2 divise l'autre ; donc $y' = \pm u^2$. De même, avec z' et x'. L'équation peut donc s'écrire $\pm u^7 \pm v^7 \pm w^7 = 0$. Si donc l'équation proposée était soluble, celle-ci le serait ; or, celle-ci est insoluble ; donc, la première l'est également (1).

§ XVIII. — Sur le dernier théorème de Fermat, par le professeur Dickson (1908-1909).

L'auteur suppose que $u^n + v^n + w^n = 0$ a des solutions premières à n. Il part des formules de Legendre $v + w = a^n$, $\varphi(v, w) = \alpha^n$, $u = -a\alpha$, etc.

(1) Dans l'*Arithmétique sur les courbes algébriques*, A. Weil indique les auteurs à consulter : Nöther, *Mathematische Annalen*, Bd. 23 ; *Ueber der Diophantischen Gleichungen vom Geschlecht null*, von Hilbert und Hurwitz in Königsberg (*Acta mathematica*, t. XIV, p. 217 (1890)) ; H. Poincaré (*Liouville*, 5e série, t. XVII, p. 161 (1901)) ; il démontre que sur toute courbe unicursale il existe une infinité de points rationnels ; il passe ensuite aux courbes de genre *un* ; il dit que $x^3 + y^3 + z^3 = 0$ n'a comme points rationnels que ses points d'inflexion, (1, — 1, 0), etc. ; Mordell, *Philos. soc.*, t. XXI (1922) ; Nogell, Gauthier-Villars, Paris.

« THÉORÈME. *S'il y a un nombre impair premier p tel que la congruence* $\xi^n + \eta^n + \zeta^n \equiv 0$ *(mod. p) n'a pas de solutions entières* ξ, η, ζ, *chacune non divisible par p, et tel que n n'est pas le résidu de la* $n^{ième}$ *puissance d'un entier (mod. p), l'équation proposée* $u^n + v^n + w^n = 0$ *n'a pas de solutions entières premières à n.*

« En effet, si u, v, w satisfont à cette équation, ils satisferont aussi à la congruence. Donc, l'un d'eux, u, sera divisible par p ; sinon la congruence n'aurait pas de solution.

« D'après une des équations de Legendre $2u = b^n + c^n - a^n$, on a $b^n + c^n + (-a)^n \equiv 0$ (mod. p). Donc a, b ou c est divisible par p. »

L'auteur montre que c'est a ; d'où $a \equiv 0$, $u \equiv 0$, $w \equiv -v$, $\varphi(u, v) \equiv v^{n-1}$, $\varphi(v, w) \equiv nv^{n-1}$ (mod. p).

On déduit de ces relations et des formules de Legendre que $\gamma^n \equiv v^{n-1}$, $\alpha^n \equiv nv^{n-1}$, d'où $n\gamma^n \equiv \alpha^n$, qui s'écrit $n \equiv (\alpha\gamma_1)^n$, γ_1 étant déterminé par $\gamma\gamma_1 \equiv 1$ (mod. p). Or, cette dernière valeur de n est en opposition avec l'énoncé du théorème.

Le théorème étant démontré, faisons voir que la congruence de l'énoncé n'a pas de solutions entières, aucune des inconnues n'étant divisible par p.

En effet, si elle en avait, déterminons r par $r\xi \equiv 1$ (mod. p) et multiplions la congruence par r^n ; nous en obtenons une autre de forme $1 + r^n \equiv s^n$ (mod. p), qui a des solutions entières non congrues à zéro.

D'après Fermat, on a $r^{mn} \equiv 1$, $s^{mn} \equiv 1$ (mod. $mn + 1$ ou p). Posons $r^n = z$; alors les congruences $z^m \equiv 1$, $(1 + z)^m \equiv 1$ ont une solution commune, z. Réciproquement, d'une solution commune, z, nous pouvons déduire des solutions entières, r, s, non congrues à zéro, et, par suite, des solutions pareilles de $\xi^n + \eta^n + \zeta^n \equiv 0$.

L'auteur étudie maintenant les deux congruences en z. Il examine successivement des valeurs particulières de m, n, et aboutit à des conclusions telles que celle-ci : quand n et $56n + 1$ ou p sont premiers, la congruence en ξ, η, ζ n'a pas de solutions entières, chacune des inconnues première

à n (mod. p), excepté quand $n=3$, 7, 229, 337, 757.

Dans un second mémoire, suite du premier, l'auteur aboutit à des conclusions applicables à $n<6857$.

§ XIX. — Du dernier théorème de Fermat, par A. Wieferich (1909).

L'auteur part de l'identité

$$te^{v}-t^{p}e^{pv}=(1+te^{v})\sum_{i=1}^{p-1}(-1)^{i-1}t^{i}e^{iv}.$$

« La $x^{ième}$ dérivée par rapport à v donne pour $v=0$

$$t-t^{p}p^{x}=(1+t)\varphi_{x+1}+\binom{x}{1}t\varphi_{x}+\binom{x}{2}t\varphi_{x-1}+\cdots+\binom{x}{x-1}t\varphi_{2}+\binom{x}{x}t\varphi_{1}.$$

« Si je pose $\frac{1+t}{t}=\delta$, j'obtiens facilement le système d'égalités

$$\delta\varphi_{x+1}+\binom{x}{1}\varphi_{x}+\cdots+\binom{x}{x}\varphi_{1}=1-t^{p-1}p_{x},$$

$$\delta\varphi_{x}+\binom{x-1}{1}\varphi_{x-1}+\cdots+\binom{x-1}{x-1}\varphi_{1}=1-t^{p-1}p^{x-1},$$

. . . .,

$$\delta\varphi_{2}+\varphi_{1}=1-t^{p-1}p.$$

$$\delta\varphi_{1}=1-t^{p-1}. \text{ »}$$

Entre ces $p+1$ égalités l'auteur élimine φ_x, ... φ_1, et obtient une relation telle que $\delta^{x+1}\varphi_{x+1}=\Delta$, où Δ est un déterminant dont une colonne est formée des seconds membres des $p+1$ égalités.

A la suite de plusieurs transformations effectuées sur Δ, l'auteur parvient à la congruence

$$-\delta\varphi_{p-1}\equiv-2B_{p-1}+(2-\delta)\left[C_{p-2}^{2}B_{\frac{p-3}{2}}\frac{2^{p-3}-1}{\frac{p-3}{2}}\varphi_{3}+\cdots+C_{p-2}^{p-3}B_{1}(2^{2}-1)\varphi_{p-2}\right] \pmod{p}.$$

« Nous allons maintenant supposer que les congruences $\varphi_3 B_{\frac{p-3}{2}} \equiv 0, \ldots, \varphi_{p-2} B_1 \equiv 0$ soient toutes vérifiées. Alors la congruence se réduit à $\delta\varphi_{p-1} \equiv B_{p-1}$. Or on a

$$\varphi_{p-1} \equiv \sum_{j=1}^{p-1} (-1)^{j-1} t^j j^{p-2} \quad \text{(Mirimanoff)},$$

c'est-à-dire

$$\varphi_{p-1} \equiv t - \frac{1}{2} t^2 + \frac{1}{3} t^3 \cdots - \frac{1}{p-1} t^{p-1}$$

$$\equiv \frac{1}{p} [C_p^1 t + C_p^2 t^2 + \cdots + C_p^{p-1} t^{p-1}],$$

$$\varphi_{p-1} \equiv \frac{(1+t)^p - 1 - t^p}{p} \quad (\text{mod. } p).$$

« On peut maintenant montrer facilement qu'on doit avoir $\varphi_{p-1} \equiv 0$, c'est-à-dire $(1+t)^p - 1 - t^p \equiv 0 \pmod{p^2}$.

« t est égal, par exemple, à $\frac{y}{x}$. Comme $x+y+z \equiv 0 \pmod{p}$, cette co‹gruence s'écrit $\frac{(Ap-z)^p - x^p - y^p}{px^p} \equiv 0 \pmod{p}$. Elle est donc vérifiée.

« Il en résulte que $B_{p-1} \equiv 0 \pmod{p}$. Or,

$$B_{p-1} \equiv 1 - \frac{1}{2} + \frac{1}{3} \cdots - \frac{1}{p-1}$$

$$= \frac{1}{p} [C_p^1 + C_p^2 + \cdots + C_p^{p-1}] \equiv \frac{2^p - 2}{p} \quad (\text{mod. } p).$$

Comme les valeurs $t \equiv 0$, $t \equiv -1$ ne sont pas considérées d'après l'hypothèse que x, y, z sont premiers avec p, il s'ensuit que satisfaire à la congruence $\varphi_i B_{\frac{p-i}{2}} \equiv 0 \pmod{p}$ entraîne la congruence $2^{p-1} \equiv 1 \pmod{p^2}$. »

§ XX. — Remarque sur le grand théorème de Fermat,

par A. Fleck (1909).

L'auteur part des formules de Legendre

$$y + z = a^p, \quad y^{p-1} - zy^{p-2} + \cdots = \alpha^p, \quad x = -a\alpha, \quad \text{etc.}$$

Bornons-nous ici au cas de x, y, z non divisibles par p.

Il signale de nouvelles propriétés. Ainsi, si $D(y, z) = 1$, $\frac{y^p + z^p}{y+z}$ n'a que des facteurs de la forme $2\mu p + 1$; $s = x + y + z$ est divisible par p^3 ; α, β, γ n'ont que des facteurs $2\mu p^2 + 1$; $x^{p-1} \equiv 1 \pmod{p^3}$, ainsi que y^{p-1} et z^{p-1}.

La différence, Q, $y^{p-1} - zy^{p-2} \cdots + z^{p-1} - (y+z)^{p-1}$, est divisible par $y^2 + yz + z^2$ ou par $(y^2 + yz + z^2)^2$ suivant que $p = 6m \mp 1$. Les trois trinomes tels que $y^2 + yz + z^2$ admettent avec s le même p. g. c. d., d'où leurs expressions GJ, GK, GL.

Les expressions telles que $x^{2p} - y^p - z^p$, quand on suppose $x^p + y^p + z^p = 0$, s'écrivent aussi GJ_1, GK_1, GL_1.

L'auteur termine ainsi son mémoire : « Nous avons appris à connaître une grande série de nombres qui ne se composent que de facteurs $6\mu + 1$, ou $3\mu + 1$, ou $2\mu p^2 + 1$. Ceux-ci sont A, B, C, φ, J, ... L_1, premiers deux à deux.

« Le problème serait, comme il est facile de le voir, complètement résolu si on pouvait montrer qu'une des grandeurs α, β, γ est égale à 1, ou que deux grandeurs J,... L_1 sont égales à 1. »

Dans un second mémoire, il commence ainsi : « Je vais montrer aujourd'hui que ces six grandeurs se composent de facteurs $6\mu p^2 + 1$. »

§ XXI. — Sur le dernier théorème de Fermat et sur le critérium de M. Wieferich,

par D. Mirimanoff (*Enseignement mathématique*, 1909-10).

« L'importance du résultat obtenu par M. A. Wieferich n'échappera à personne: l'impossibilité de l'équation de Fermat se trouve ainsi démontrée pour tous les nombres premiers p tels que $2^{p-1} - 1$ ne soit pas divisible par p^2, en particulier pour tous les nombres de Mersenne et leurs analogues et pour tous les nombres premiers p pour lesquels la division du cercle en p parties égales peut se faire avec la règle et

le compas, en supposant toutefois xyz non divisible par p.

« Cette importance m'a déterminé à reprendre les congruences générales employées par M. Wieferich. On ne peut pas ne pas être frappé de l'analogie que présente la dernière avec la formule connue d'Euler donnant la somme alternée des puissances des premiers nombres entiers.

« Je démontrerai que la congruence est une conséquence de la formule.

« *Congruences fondamentales* de Kummer. Désignons par $\varphi_i(t)$ ou φ_i le polynome $t - 2^{i-1}t^2 + 3^{i-1}t^3 \cdots - (p-1)^{i-1}t^{p-1}$, en faisant $i = 1, 3, \ldots (p-2)$, et aussi $i = p-1$.

« Supposons maintenant que l'équation de Fermat admette une solution première à p. Soit t l'un des rapports $\frac{x}{y} \ldots$ ou, ce qui revient au même, son reste (mod. p) ; le nombre t n'est congru ni à 0 ni à -1 (mod. p). Voici donc comme s'énonce le critérium qui résulte des recherches de Kummer et que je voulais rappeler : Chacun des six rapports t vérifie le système des congruences

(1) $B_{\frac{p-i}{2}} \varphi_i(t) \equiv 0$ (mod. p), $i = 3, 5, \ldots (p-2)$ auxquelles adjoignons

(2) $\varphi_{p-1}(t) \equiv 0$, qui résulte de (1) ; donc, en tout, $\frac{p-1}{2}$ congruences.

« *Congruence de Wieferich.* Établissons-la comme il a été dit. »

L'auteur part de l'égalité

$$1 - 2^{2n+1} + 3^{2n+1} + \cdots + (-1)^{y+1} y^{2n+1}$$
$$= (-1)^{y+1} \left\{ \frac{1}{2} y^{2n+1} + \binom{2n+1}{1} \frac{2^2-1}{2} B_1 y^{2n} \right.$$
$$- \binom{2n+1}{3} \frac{2^4-1}{4} B_2 y^{2n-2} + \cdots (-1)^{n-1} \binom{2n+1}{2n-1} \frac{2^{2n}-1}{2n} B_n y^2$$
$$\left. + (-1)^n \frac{2^{2n+2}-1}{2n+2} B_{n+1} \right\} + (-1)^n \frac{2^{2n+2}-1}{2n+2} B_{n+1}$$

(*Cf. L. Saalschütz, Vorlesungen über die Bernoullischen Zahlen*, p. 53), et, à la suite de quelques calculs, il en déduit

l'identité en t

$$[1-2^{p-2}+\cdots-(p-1)^{p-2}]t^p-\frac{1}{2}(t+1)\varphi_{p-1}$$
$$=(t-1)\Big\{\binom{p-2}{1}\frac{2^2-1}{2}B_1\varphi_{p-2}-\binom{p-2}{3}\frac{2^4-1}{4}B_2\varphi_{p-4}$$
$$+\cdots+(-1)^{\frac{p-5}{2}}\binom{p-2}{p-4}^{p-1}\frac{2^{p-3}-1}{p-3}B_{\frac{p-3}{2}}\varphi_3\Big\}$$
$$+(-1)^{p-1}\frac{2^p-2}{p-1}B_{\frac{p-1}{2}}\frac{t^p-t}{t+1}.$$

Si maintenant on envisage cette identité comme une congruence (mod. p), on a le droit de supprimer le dernier terme à la condition que t soit différent de -1 (mod. p). En effet, le facteur p qui figure au dénominateur de $B_{\frac{p-1}{2}}$ disparaît en multipliant par 2^p-2, et, d'autre part, t^p-1 s'annule pour toutes les valeurs entières de t (mod. p).

Mais en supprimant le dernier terme de l'identité, on obtient précisément la dernière congruence de laquelle Wieferich a tiré son critérium (loc. n° 3, form. 18).

On voit donc que la congruence de Wieferich résulte de l'identité, laquelle est une conséquence de la formule d'Euler. Mais la réciproque n'est pas vraie ; il ne serait pas facile de déduire l'identité de la congruence de Wieferich.

Supposons maintenant que l'équation de Fermat soit possible en nombres entiers premiers à p. Il existera alors une et même plusieurs racines t, différentes de 0 et de -1, qui annuleront les premiers membres des congruences (1) et (2). L'identité se réduira à son premier terme et nous aurons la condition

$$1-2^{p-2}+\cdots-(p-1)^{p-2}\equiv 0 \quad (\text{mod. } p).$$

Or, le premier membre de cette congruence est congru à $\frac{2^p-2}{p}$ (mod. p) (*Cf.* P. Bachmann, *Niedere Zahlentheorie*, p. 163). D'où $\frac{2^{p-1}-1}{p}\equiv 0$ (mod. p).

§ XXII. — **Sur le théorème de Fermat,**

par G. Frobenius (1909-10).

Soit p un nombre premier impair ; soient x, y, z trois nombres entiers non divisibles par p, satisfaisant à l'équation de Fermat $x^p + y^p + z^p = 0$.

On a alors

(1) $$x + y + z \equiv 0 \pmod{p},$$

comme il est à compter dans ce qui suit, avec

$$(x+y)^p \equiv -z^p = x^p + y^p \pmod{p^2}.$$

Je pose

(2) $$\varphi_n(t) = \sum_r r^{n-1}(-t)^r,$$

où r varie de 0 à $p-1$ (tiré de M. Mirimanoff),

(3) $$\varphi_1(t) = \Sigma(-t)^r = \frac{1+t^p}{1+t};$$

alors, si n varie de 1 à $p-1$,

$$\varphi_{p-1}(t) \equiv \sum_n \frac{1}{n}(-t)^n \equiv -\frac{1}{p}\sum \binom{p}{n} t^n$$

et, en même temps,

(4) $$\varphi_{p-1}(t) \equiv \frac{1}{p}\left[1 + t^p - (1+t)^p\right].$$

A la formule précédente satisfont par conséquent les six nombres $\frac{x}{y}$, $\frac{y}{x}$, $\frac{x}{z}$, $\frac{z}{x}$, $\frac{y}{z}$, $\frac{z}{y}$ (mod. p) de la congruence

(5) $$\varphi_{p-1}(t) \equiv 0.$$

De ces nombres, aucun n'est égal à 0, et, d'après (1), aucun n'est égal à -1.

En outre, ils satisfont encore, d'après Kummer, à $\frac{1}{2}(p-3)$ congruences, que M. Mirimanoff a mises sous la forme

(6) $$B_{2k}\varphi_{p-2k}(t) \equiv 0 \qquad (2k = 2, 4, \ldots p-2).$$

Ici, $B_2 = \frac{1}{6}$, $B_4 = \frac{1}{30}$ ... sont les nombres de Bernoulli.

Des conditions (5) et (6) M. Wieferich a tiré d'une manière très perspicace la congruence

$$(7) \qquad 2^{p-1} \equiv 1 \pmod{p^2},$$

dans son travail sur le dernier théorème de Fermat (*Journal de Crelle*, t. CXXXVI, p. 293), auquel je renvoie.

A ce résultat, qui est précieux pour sa facilité d'être utilisé par le calcul, on peut arriver simplement par le moyen suivant.

La double somme

$$(8) \qquad L = \sum_{r,s} (-1)^{r-2}(r-s)^{p-2}t^2,$$

où r et s varient de 0 à $p-1$, est

$$L = \sum_{n,r,s} (-1)^n \binom{p-2}{n-1} (-1)^r r^{n-1} (-1)^s s^{p-n-1} t^s.$$

où $r^{n-1} = 1$, à moins que $r = n - 1 = 0$.

Par suite $L = \sum_n (-1)^n \binom{p-2}{n-1} \varphi_n(1) \varphi_{p-n}(t)$.

D'après (3), $\varphi_1(t)^n \equiv 1$. Plus loin,

$$0 < k < \frac{1}{2}(p-1),$$

$$\varphi_{2k+1}(1) = \Sigma(-1)^n n^{2k} \equiv 0,$$

$$\varphi_{2k}(1) = \Sigma(-1)^n n^{2k-1} \equiv (-1)^k B_{2k} \frac{1}{k}(2^{2k} - 1).$$

La première congruence est vérifiée en remplaçant n par $p - n$; la deuxième

$$S_n\left(\frac{1}{2}(p+1)\right) \equiv S_n\left(\frac{1}{2}\right),$$

où

$$S_n(x) \equiv \frac{1}{n+1} x^{n+1} - \frac{1}{2} x^n + \cdots$$

est la fonction de Bernoulli. D'après (5) et (6), on a, par

conséquent,

$$(9)\qquad L \equiv \varphi_{p-1}(1).$$

Maintenant, je décompose la somme (8) en deux sommes partielles $M+N$, en distinguant si $r-s$ est positif ou négatif; si $r-s=n>0$, alors

$$M = \Sigma(-1)^n n^{p-2}(1+t+\cdots+t^{p-1-n}),$$

$$\begin{aligned}(1-t)M &= \Sigma(-1)^n n^{p-2}(1-t^{p-n})\\ &\equiv \varphi_{p-1}(1) - \Sigma(-1)^{p-n}(1+n)^{p-2}t^{p-n},\end{aligned}$$

ou, si on remplace $p-n$ par n,

$$(1-t)M \equiv \varphi_{p-1}(1) - \varphi_{p-1}(t) \equiv \varphi_{p-1}(1).$$

Mais, si $r-s=-n<0$, alors

$$N = -\Sigma(-1)^n n^{p-2}(t^n+t^{n+1}+\cdots+t^{p-1}),$$

$$\begin{aligned}(1-t)N &= -\Sigma(-1)^n n^{p-2}(t^n-t^p)\\ &\equiv -\varphi_{p-1}(t) + t^p\varphi_{p-1}(1) \equiv t\varphi_{p-1}(1)\end{aligned}$$

et, par conséquent,

$$(1-t)L \equiv (1+t)\varphi_{p-1}(1).$$

Si on compare ce résultat à la formule (9), on obtient la congruence $\varphi_{p-1}(1) \equiv 0$, qui est, d'après (4), la même chose que la relation (7).

§ XXIII. — **Note sur le dernier théorème de Fermat,**

par D. Mirimanoff (1910).

L'auteur débute comme dans *l'Enseignement mathématique* (§ XXI). Il montre que les polynomes $\varphi_i(t)$ sont liés par une relation. En y faisant $t=-1$, il la réduit à

$$q(m) = \sum_{i=1}^{m-1} \frac{R_i}{1-\alpha_i},$$

où $\alpha_1, \alpha_2, \ldots \alpha_{m-1}$ sont les racines de $\dfrac{z^m-1}{z-1}$, m un nombre premier quelconque. On a posé $R_i(1-\alpha_i)^{p-1} = \varphi_{p-1}(-\alpha_i)$.

L'auteur remarque que cette formule fournit l'expression générale du quotient de Fermat.

A la suite d'un dernier calcul, il obtient la congruence

$$\prod_{i=1}^{m-1}(t+\alpha_i)\cdot\sum_{i=1}^{m-1}\frac{R_i}{t+\alpha_i}\equiv 0 \pmod{p},$$

Π désigne un produit.

« On peut donc énoncer le théorème suivant : Si

$$x^p+y^p+z^p=0,$$

chacun des six rapports tels que $\frac{x}{y}$ vérifie la congruence précédente.

En y faisant $m=2$, on retrouve la relation de Wieferich.

Pour $m=3$, la congruence s'écrit

$$R_1+R_2+\alpha_2R_1+\alpha_1R_2\equiv 0$$

et comme le nombre des rapports distincts $\frac{x}{y}$ (mod. p) est au moins égal à 2, on doit avoir

$$R_1+R_2\equiv 0, \qquad \alpha_2R_1+\alpha_1R_2\equiv 0,$$

d'où

$$q(3)\equiv 0.$$

On voit que l'impossibilité de $x^p+y^p+z^p=0$ est établie, dans le cas où x, y, z sont premiers à p, pour tous les exposants premiers p tels que l'un au moins de $q(2)$, $q(3)$ ne soit pas divisible par p.

Elle est établie, en particulier, pour tous les exposants premiers de la forme $2^a.3^b\pm 1$ et de la forme $\pm 2^a\pm 2^b$.

D'autres critériums peuvent être déduits de l'expression générale de $q(m)$, en donnant à m des valeurs supérieures à 3. »

CHAPITRE XI

DE MIRIMANOFF A 1931

§ I. — Le dernier théorème de Fermat démontré, par L. Gouy (1912).

Posant $(x+y)^n - x^n - y^n = z$, l'équation s'écrit

$$\frac{z^n}{(x+y)^n} + \frac{z}{(x+y)^n} = 1.$$

Evidemment $x+y$ et z ne sont pas premiers entre eux ; soit d leur p. g. c. d., d'où $z = ad$, $x+y = bd$, et, par suite, $\left(\frac{a}{b}\right)^n + \left(\frac{z}{bd}\right)^n = 1$.

Cette dernière relation serait donc impossible, si la seconde fraction, réduite à sa plus simple expression, n'avait pas b^n pour dénominateur.

§ II. — Démonstration du théorème de Fermat, par E. Fabry (1913).

« Soit α une racine imaginaire de $\alpha^\lambda = 1$, λ, premier ; $f(\alpha)$, un nombre complexe idéal quelconque ; k, un nombre entier positif, inférieur à λ.

« On considère les entiers positifs, h, inférieurs à λ, tels que la somme de h et du résidu positif de kh (mod. λ) soit supérieure à λ. Il y en a $\frac{\lambda - 1}{2}$. A chacun on fait correspondre un entier m_h tel que $h . m_h \equiv 1$ (mod. λ).

« Kummer prouve que, quel que soit α, le produit des $\frac{\lambda-1}{2}$ nombres idéaux conjugués $f(\alpha^{m_h})$ est toujours un nombre complexe existant (non idéal).

« Soient x, y, z, non divisibles par λ, vérifiant

$$x^\lambda + y^\lambda + z^\lambda = 0.$$

On a $(-z)^\lambda = (x+y)(x+\alpha y)\ldots(x+\alpha^{\lambda-1}y)$; ces derniers facteurs sont premiers entre eux deux à deux ; par conséquent, chacun d'eux est le produit d'une unité complexe par la puissance $\lambda^{ième}$ d'un nombre complexe existant ou idéal ; d'où la congruence

$$(x+\alpha^{n_1}y)(x+\alpha^{n_2}y)\ldots(x+\alpha^{n_\mu}y) \equiv \alpha^r \mathrm{E}(\alpha)\mathrm{Q}^\lambda(\alpha), \text{ (mod. } \lambda), \quad (1)$$

$n_1, n_2 \ldots n_\mu$ étant les μ nombres m_h de Kummer. »

L'auteur la transforme successivement en deux autres, dont le second membre est $\mathrm{A}\alpha^r$, A nombre entier réel, et

$$(x+y)^\mu \alpha^{t\mathrm{N}\mu}, \qquad t = \frac{y}{x+y}, \qquad \mathrm{N} = n_1 + n_2 + \cdots + n^\mu.$$

Le produit des μ facteurs du premier membre effectué, l'auteur parvient à déduire de la dernière congruence, celle-ci : $\Sigma(n^2 + n^3 + \cdots + n^{\lambda-2}) \equiv 0$ (mod. λ) et comme,

$$n^2 + n^3 + \cdots + n^{\lambda-2} \quad \text{ou} \quad \frac{n^{-1} - n^2}{n-1}$$

est congru à $-n-1$ (mod. λ), on a

$$n_1 + n_2 + \cdots + n_\mu + \mu \equiv 0 \text{ (mod. } \lambda).$$

Or, pour $k = 1$, les h sont $\mu+1, \mu+2, \ldots 2\mu$;
pour $k = \mu$, les h sont $2, 4, 6 \ldots 2\mu$.

Pour ces deux valeurs de k, la congruence précédente donne

$$\frac{1}{\mu+1} + \frac{1}{\mu+2} + \cdots + \frac{1}{2\mu} + \mu \equiv 0,$$

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{\mu} + 2\mu \equiv 0$$

et, par addition de celles-ci,

$$1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{\mu}+\frac{1}{\mu+1}+\cdots+\frac{1}{2\mu}+3\mu\equiv 0.$$

Or, $$\frac{1}{p}+\frac{1}{2\mu-p+1}=\frac{\lambda}{p(2\mu-p+1)}\equiv 0.$$

Donc, il reste $3\mu\equiv 0$, qui n'est possible que pour $\lambda=3$. »

Supposons maintenant que y soit divisible par λ.

La congruence (1) est remplacée par l'égalité

$$(x+\alpha^{n_1}y)\ldots(x+\alpha^{n_\mu}y)=Q^\lambda(\alpha).$$

Comme dans le premier cas, l'auteur parvient à une dernière congruence, $y\equiv 2x(1-x^{2\mu^2})$ (mod. λ^2). Donc y doit être divisible par λ^2.

« *L'égalité $x^\lambda+y^\lambda+z^\lambda=0$ est donc impossible :*

1° *Si x, y, z ne sont pas divisibles par λ;*

2° *Si l'un d'eux est divisible par λ, sans l'être par λ^2.* »

§ III. — Sur la résolution de $x^n+y^n=z^n$,

par Joseph Joffroy (1911).

« Fermat a établi l'égalité $a^p=mp+a$, p étant premier, a, m entiers quelconques.

« Généralisée, elle s'écrit $a^{p+k(p-1)}=mp+a$, k entier quelconque. Appliquons-la à $x^{37}+y^{37}=z^{37}$ (1).

« Elle fournit aisément

$$x^{37}=\begin{cases}2m+x,\\3m+x,\\5m+x,\\7m+x,\\13m+x,\\19m+x,\\37m+x.\end{cases}$$

« Donc $x^{37}-x$, qui est multiple de 2, 3, ..., 37, est multiple

de leur produit P. On peut donc écrire

$$x^{37} - x = \mathrm{P}m, \quad y^{37} - y = \mathrm{P}m', \quad z^{37} - z = \mathrm{P}m'',$$

d'où, en tenant compte de (1), $x + y - z = \mathrm{P}m_1$.

« Il est aisé de prouver que $\mathrm{P}m_1$ est positif. On a donc, si $x < y < z$, $x > \mathrm{P} + 1$, ou $x > 1919191$.

« *Conclusion.* — Si l'équation $x^{37} + y^{37} = z^{37}$ admet des solutions entières, elles sont supérieures à ce nombre, ce qui n'incite pas à penser que cette équation en admet.

« On tire aussi aisément de la formule de départ :

$$a^{85} = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 29 \cdot 85m + a = 6729450m + a,$$
$$a^{49} = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 49m + a = 2274090m + a,$$

et j'en conclus, comme ci-dessus, pour les solutions entières des équations correspondantes de Fermat, supposées possibles, des nombres considérables.

« La même remarque est applicable à autant d'équations de Fermat qu'on voudra. »

§ IV. $x^2 + y^2 = z^2$, $x^4 + y^4 = z^2$, $x^4 + y^4 = z^4$, $x^3 + y^3 = z^3$, par Eugène Cahen (1924).

1° $x^2 + y^2 = z^2$.

« Une méthode de discussion consiste à trouver les points à coordonnées rationnelles de $\mathrm{X}^2 + \mathrm{Y}^2 = 1$.

« Appliquons-la à l'équation $x^2 + y^2 = (a^2 + b^2)z^2$. On pose $\frac{y}{z} - b = \frac{t}{u}\left(\frac{x}{z} - a\right)$ et on trouve $x = \frac{-at^2 + 2btu + au^2}{\mathrm{D}}$, $y = \frac{bt^2 + 2atu - bu^2}{\mathrm{D}}$, $z = \frac{t^2 + u^2}{\mathrm{D}}$, D étant le p. g. c. d. des numérateurs. »

L'auteur remarque que $x^2 + y^2 = \mathrm{A}z^2$ n'a pas de solution si A n'est pas la somme de deux carrés.

« En effet, soit x_0, y_0, z_0 une solution, où $\mathrm{D}(x_0, y_0, z_0) = 1$. Soit d le p. g. c. d. de x_0 et y_0 ; $x_0 = dx_1$, $y_0 = dy_1$; d'où $d^2(x_1^2 + y_1^2) = \mathrm{A}z_0^2$. d^2 divise A ; soit $\mathrm{A} = d^2\mathrm{A}'$; d'où

$x_1^2 + y_1^2 = A' z_0^2$. D'après ce théorème: Si un entier est la somme de deux carrés, premiers entre eux, il en est de même de tout diviseur de cet entier, l'entier A′ est une somme de deux carrés, et il en est de même de A. »

$$2^\circ \quad x^4 + y^4 = z^2.$$

« On peut supposer x, y, z premiers deux à deux. Transformant l'égalité en congruence (mod. 4), on voit que x et y ne peuvent être impairs. Soit $x = 2^n x'$, d'où $2^{4n} x'^4 + y^4 = z^2$.

« Nous allons faire la démonstration pour $\varepsilon \, . \, 2^n x^4 + y^4 = z^2$, plus générale. Elle s'écrit $\varepsilon \, . \, 2^{2n} x^4 = (z + y^2)(z - y^2)$. Le p. g. c. d. des deux derniers facteurs est 2. Donc, on a, par exemple, $z - y^2 = \varepsilon' 2 u^4$, $z + y^2 = \varepsilon'' 2^{2n-1} v^4$, ε, ε', ε'' sont ± 1 ; u, v, premiers relatifs. Une autre combinaison se ramène à celle-ci. On en tire $y^2 = \varepsilon'' 2^{2n-2} v^4 - \varepsilon' u^4$.

« Si $n > 1$, cette équation, transformée en congruence (mod. 4), donne $1 \equiv -\varepsilon'$. Donc $\varepsilon' = -1$, et l'équation devient $\varepsilon'' 2^{2n-2} v^4 = y^2 - u^4$ semblable à celle de départ, l'exposant de 2 diminué de 2.

« En répétant ce procédé autant de fois qu'il est nécessaire, on arrive à une équation semblable où l'exposant est 1.

« Soit $4\varepsilon \, . \, x^4 = z^2 - y^4$, x, y, z impairs. Or, en transformant celle-ci en congruence (mod. 4), on voit qu'elle est impossible.

« Le théorème de Fermat est donc vrai pour $n = 4$ et $n = 4m$. »

$$3^\circ \quad x^3 + y^3 + z^3 = 0.$$

L'auteur établit d'abord deux lemmes :

I. *Si l'on a* $x^2 - xy + y^2 = u^3$, *avec* $D(x, y) = 1$, *l'un des nombres* x, y, $x - y$ *est divisible par* 6.

II. *Sur les trois valeurs de* x, y, z *constituant une solution primitive* (x, y, z *premiers entre eux deux à deux*), *il y en a une qui est divisible par* 6.

« Soit donc $z = -2^m \, . \, 3^n t$. On a

$$(x + y)(x^2 - xy + y^2) = 2^{3m} 3^{3n} t^3,$$

x, y, t n'étant divisibles ni par 2, ni par 3.

« Cherchons comment les facteurs 2, 3 se distribuent dans le premier membre. » On trouve

$$x+y=2^{3m}3^{3n-1}u^3, \qquad x^2-xy+y^2=3v^3.$$

« La seconde équation s'écrit

$$\left(\frac{2x-y}{3}\right)^2-\frac{2x-y}{3}\frac{x+y}{3}+\left(\frac{x+y}{3}\right)^2=v^3. \text{ »}$$

L'auteur en déduit l'expression de v et ensuite celle de $x+y$, d'où les équations

$$v=\xi^2-\xi\eta+\eta^2, \qquad \xi\eta(\xi-\eta)=2^{3m}3^{3(n-1)}u^3,$$

qui donnent

$$\xi=q^3, \qquad \eta=-r^3, \qquad \xi-\eta=-s^3, \qquad qrs=2^m3^{n-1}u.$$

« On a alors $q^3+r^3+s^3=0$ semblable à l'équation de départ; mais celle des inconnues qui contiendrait 3 le contiendrait avec un exposant diminué de 1.

« De proche en proche, on arriverait à des solutions ne contenant pas le facteur 3 ; ce qui est impossible. »

4° $X^4+Y^4=Z^2$ en nombres $a+bi$.

Lemme. — *Si* A *est un entier non divisible par* $1-i$, *on a :*

si	$A\equiv 1$ (mod. 2),	$A^2\equiv 1$ (mod. 4);
si	$A\equiv i$ (mod. 2),	$A^2\equiv -1$ (mod. 4);
dans tous les cas,		$A^4\equiv 1$ (mod. 8).

Soit maintenant $x^4+y^4=z^2$. On peut se borner aux solutions primitives.

Si aucune inconnue n'était divisible par $1-i$, l'équation, transformée en congruence (mod. 2), donnerait $2\equiv 1$.

Ce n'est pas z. En effet, si on avait $z=(1-i)^\alpha z'$, on aurait la congruence (mod. 8): $2\equiv(1-i)^{2\alpha}z'^2$ ou $1\equiv(-i)^\alpha z'^2$ (mod. 4). Ce qui exige d'abord $\alpha=1$, ensuite $1\equiv\pm i$ (mod. 4), ce qui n'est pas.

Supposons que ce soit x; remplaçons x par $(1-i)^n x$; d'où

l'équation

$$(1-i)^{4n}x^4+y^4=z^2, \quad \text{ou} \quad (-4)^n x^4+y^4=z^2.$$

Nous allons traiter l'équation plus générale $\varepsilon 4^n.x^4+y^4=z^2$, $\varepsilon=\pm 1$ ou $\pm i$.

Je dis d'abord que $z\equiv 1$ (mod. 2). En effet, dans le cas contraire, on aurait $z\equiv i$ (mod. 2), et il en résulterait $0\equiv -1-1$ (mod. 4), ce qui n'est pas.

Je dis maintenant que $n>1$. En effet, soit $z=2t+1$; d'où $z^2=4t(t+1)+1$. L'un des deux entiers t ou $t+1$ est divisible par $1-i$; donc $z^2\equiv 1$ [mod. $(1-i)^5$]. — Quant à y^4, il est congru à 1 (mod. 8). On voit ainsi que le second membre de l'équation est divisible par $(1-i)^5$. Donc, le premier membre l'est aussi, et, par suite, $n>1$.

L'équation s'écrit $\varepsilon . x^4=(z-y^2)(z+y^2)$.

Le p. g. c. d. des deux facteurs, divisant $2z$ et $2y^2$, ne peut être que $1-i$ ou 2. C'est 2, parce que z et y^2 sont congrus à 1 (mod. 2).

L'équation donne alors $z-y^2=\eta . 2 . u^4$, $z+y^2=\eta_1 2^{2n-1}v^4$, ou $z-y^2=\eta_1 2^{2n-1}v^4$, $z+y^2=\eta . 2u^4$, η et η_1 étant des unités ± 1, $\pm i$.

Le second système se ramène au premier si on change y en iy. Du premier, on tire $y^2=\eta_1 2^{2n-2}v^4-\eta u^4$, qui donne $\eta\equiv\pm 1$ (mod. 4). Donc on a soit $\eta_1 2^{2n-2}v^4=y^2-u^4$, soit $\eta_1 2^{2n-2}v^4=y^2+u^4$.

La seconde équation se ramène à la première, si on change η_1 en $-\eta_1$ et y en iy.

La première est semblable à la proposée, mais n est remplacé par $n-1$. En continuant ainsi, on arriverait donc à une équation semblable, où n serait égal à 1. Or, nous avons vu que c'est impossible.

Remarque. — Ce résultat contient celui de $x^4+y^4=z^2$ comme cas particulier, puisque le corps C(i) contient le corps C(1).

5° $x^3+y^3+z^3=0$ en nombres $a+bj$.

L'auteur démontre son impossibilité.

§ V. $x^n + y^n + z^n = 0$,

par Léon Pomey (1923 et 1925).

L'auteur traite les deux cas. Bornons-nous ici au premier : x, y, z premiers avec n.

Soit $X = y + z$, $p = x + X$, $S(y, z) = \frac{(y+z)^n - y^n - z^n}{nyz(y+z)}$, $P(y, z) = \frac{y^n + z^n}{y+z}$, $x^n = -PX$.

L'auteur rappelle les formules de Legendre, qu'il indique par des théorèmes :

Théorème I. $X = a^n$, $P = g^n$, $x = -ag$;

Théorème II. $p = n^v abc \cdot \varphi$;

et en établit de nouveaux :

Théorème III. On a successivement $X \equiv -x \pmod{n^v}$, $X^n \equiv -x^n \pmod{n^{v+1}}$. Par suite $(y+z)^n - y^n - z^n \equiv 0 \pmod{n^{v+1}}$, d'où $S(y, z) \equiv 0 \pmod{n^v}$.

Théorème IV. On doit avoir $v \geqslant 2$.

En effet, on a $a^n \equiv -x \pmod{n^v}$. Mais $a^n - a = kn$; donc $a \equiv -x \pmod{n}$, et, par suite, $a^n \equiv -x^n \pmod{n^2}$, d'où $\Sigma a^n \equiv 0 \pmod{n^2}$, et, comme $\Sigma a^n = \Sigma X = 2p = 2n^v abc\varphi$, v doit être au moins égal à 2.

Théorème V. On doit avoir $x^n - x \equiv 0 \pmod{n^2}$.

En effet, on a $X \equiv -x \pmod{n^v}$, où l'on fait $v = 2$, et a^n ou $X \equiv x^n \pmod{n^2}$.

Extension des derniers théorèmes. — Elle résulte de la forme $1 + 2n^\gamma\lambda$ des facteurs premiers de g, $\gamma \geqslant 2$, et de la congruence qui s'ensuit, $g \equiv 1 \pmod{n^\alpha}$, α étant le plus petit de tous les γ, correspondant aux différents facteurs et aussi à y, z comme à x.

Théorème IV ter. On doit avoir $v \geqslant \alpha + 1 \geqslant 3$, d'où $x + y + z \equiv 0 \pmod{n^3}$.

Théorème V ter. On a $x^n - x \equiv 0 \pmod{n^3}$, avec $\alpha + 1 \geqslant 3$.

Le théorème III devient alors $(y+z)^n - y^n - z^n \equiv 0 \pmod{n^4}$, $S(y, z) \equiv 0 \pmod{n^3}$.

Autre forme de ces théorèmes, si on pose $y \equiv ux$,

$z \equiv vx$ (mod. n^3): $1 + u + v \equiv 0$; $u^n - u \equiv 0$, $v^n - v \equiv 0$ (mod. n^3); $(1+u)^n - 1 - u^n \equiv 0$, $(1+v)^n - 1 - v^n \equiv 0$. $(u+v)^n - u^n - v^n \equiv 0$ (mod. n^4).

Application de ces théorèmes pour $n = 3$. 5, 59. — Les conditions nécessaires fournies par ces trois derniers théorèmes s'expriment par les congruences $x + y + z \equiv 0$, $x^n - x \equiv 0$, $S(y, z) \equiv 0$ (mod. n^3), ou $(y+z)^n - y^n - z^n \equiv 0$ (mod. n^4).

1° $n = 3$. $S(y, z)$. étant égal à 1. ne peut être divisible par 3.

2° $n = 5$. x, y, z étant premiers à 5, la première congruence exige que x ait la forme $5k \pm 1$, que y ait la forme $5k' \pm 2$, que z ait l'une d'elles. Or, la quatrième congruence se réduit à $(y+z)^2 - yz \equiv 0$ (mod. n^2), dont le premier terme vaut 1 ou 9 et l'autre ± 2. à des multiples de 5 près, et est par suite impossible.

3° $n = 59$. Rappelons que, d'après M. Arwin (*Acta mathematica*, t. XLII, 1920), la congruence $(1+u)^n - 1 - u^n \equiv 0$ a des solutions quand on prend n^2 pour module (ce qui empèche de pouvoir appliquer à ce cas le critère de Legendre). mais, au contraire. n'en a aucune si on prend n^3.

Tenant compte de ce résultat, on en déduit qu'à fortiori il n'existe pas de solution pour le module n^4. ce qui nous suffit pour conclure à *l'impossibilité de l'équation*

$$x^{59} + y^{59} + z^{59} = 0,$$

dans le premier cas.

Application des théorèmes IV, V, III bis. Ils expriment. comme nous l'avons vu, que l'équation de Fermat est impossible, dans le premier cas, si l'on peut trouver des entiers u. v de la forme $a + bn + cn^2 (a, b, c < n)$ satisfaisant aux congruences

$$1 + u + v \equiv 0, \quad u^n - u \equiv 0, \quad v^n - v \equiv 0 \quad (\text{mod. } n^3);$$
$$(u+v)^n - u^n - v^n \equiv 0, \quad (1+u)^n - 1 - u^n \equiv 0,$$
$$(1+v)^n - 1 - v^n \equiv 0 \quad (\text{mod. } n^4).$$

TABLE DE JACOBI

n	3	5	7	11	13	17	19	23	29	31	37
a	b										
1	0	0	0	0	0	0	0	0	0	0	0
2	2	1	4	10	6	9	6	11	2	12	2
3		3	4	0	11	13	16	5	16	20	17
4		4	2	7	11	2	5	21	8	17	8
5			2	2	5	9	3	1	2	14	24
6			6	8	1	2	12	20	9	14	3
7				3	11	4	15	15	22	27	25
8				10	7	6	15	17	24	20	24
9				0	1	10	1	7	7	27	28
10				10	1	12	17	11	14	26	21
11					6	14	3	8	21	13	21
12					12	7	3	14	1	7	18
13						14	6	11	22	25	13
14						3	15	15	0	14	27
15						7	13	5	28	18	9
16						16	2	7	6	12	27
17							12	2	27	16	11
18							18	21	7	7	0
19								1	14	23	36
20								17	19	17	25
21								11	4	4	9
22								22	6	3	27
23									19	10	9
24									26	3	23
25									20	16	18
26									12	16	15
27									26	13	15
28									28	10	8
29										18	12
30										30	11
31											33
32											12
33											22
34											19
35											34
36											36
37											

D'une manière générale, les congruences $u^n - u \equiv 0$, $(u+1)^n - (u+1) \equiv 0$ expriment que, parmi les racines (autres que 0 et -1) de $x^n - x \equiv 0$ (mod. n^3), doivent figurer au moins deux entiers consécutifs $u = a + bn + cn^2$.

$u+1=a+1+bn+cn^2$, faute de quoi $x^n+y^n+z^n=0$ est impossible dans le premier cas.

Pour appliquer ce principe, aidons-nous de la petite table de Jacobi ci-dessus (*Crelle*, t. III, 1828), qui donne pour $n \leqslant 37$ les racines de $x^{n-1}-1\equiv 0 \pmod{n^2}$.

Ces racines étant mises sous la forme $x=a+nb$, a, b positifs et $< n$, à chaque valeur de a la table fait correspondre la valeur appropriée de b. Pour que la condition soit réalisée, il faut donc, a étant donné, qu'il existe deux valeurs consécutives de b identiques.

Cela n'a pas lieu pour $n=3, 5, 11, 17, 23, 29$. Donc, impossibilité de l'équation $x^n+y^n+z^n=0$. Cela a lieu pour 7, 13, 19, 31, 37 (mod. n^2). Il faudrait le vérifier pour mod. n^3.

Le théorème fondamental de Sophie Germain. Critères de Legendre. Application à des valeurs de n allant jusqu'à 5 003 249.

THÉORÈME. — *L'équation* $x^n+y^n+z^n=0$ *est impossible en nombres entiers premiers à* n (1[er] *cas*) *s'il existe un nombre premier* $\theta=2kn+1$, *tel que :* 1° *la congruence* $1+\rho+\rho'\equiv 0$ (*mod.* θ) *soit impossible,* ρ, ρ' *étant deux résidus de puissances* $n^{\text{ièmes}}$ (*et, par suite, aussi, toute congruence* $u^n+v^n+w^n\equiv 0$ (*mod.* θ), *où* u, v, w *sont premiers à* θ) ; 2° n *ne soit pas un résidu de puissance* $n^{\text{ième}}$ (*mod.* θ).

De là, Legendre a déduit l'impossibilité de l'équation en nombres premiers à n, si n est tel que l'un des nombres $2n+1$, $4n+1$, $8n+1$, $10n+1$ est également premier.

Application à de grandes valeurs de n. — Nous avons cherché, entre certaines limites, les nombres premiers n qui sont tels que $2n+1$ soit encore premier. Ce sont, entre 9 043 et 10 001 : 9 049, 9 221, 9 293, 9 371, 9 419, 9 473, 9 479, 9 539, 9 629, 9 791 ; entre 5 000 000 et 5 003 371, ce sont, en ne désignant que leurs excédents sur 5 000 : 111, 263, 321, 381, 399, 741, 783, 903, 981, 1 173, 1 203, 1 299, 1 443, 1 779, 2 103, 2 223, 2 229, 2 313, 2 331, 2 583, 2 841, 3 081, 3 231, 3 249.

Nouveaux critères. — En nous appuyant, d'une part sur ces critères, d'autre part sur quelques-uns des nombreux résultats que nous avons obtenus dans la théorie des nombres premiers et que nous avons développés dans un autre Mémoire étendu, nous pouvons énoncer ces théorèmes : Impossibilité de l'équation en nombres premiers à n quand l'une des circonstances suivantes se produira :

1° Si, n étant de la forme $4k+3$, $2n+1$ divise 2^n-1.

2° Si, n étant de la forme $4k+1$, $2n+1$ divise 2^n+1.

3° Si $4n+1$ est de la forme $8k+5$ et divise $2^{2n}+1$.

4° Si $4n+1$ est de la forme $12k+5$ et divise $3^{3n}+1$.

5° Si $8n+1$ divise $2^{4n}-1$.

6° Si $10n+1$ divise $5^{5n}-1$.

§ VI. — **Mémoires de M. H.-S. Vandiver,** de Philadelphie.

Voici leurs titres :

Extension des critères de Wieferich, Mirimanoff, en connexion avec le théorème de Fermat (*Crelle*, t. CXLIV, p. 314, 1914).

Symmetric functions formed by systems of a finite algebra and their connection with Fermat's last theorem (*Annals of Mathematics*, t. XVIII, p. 105, 1916).

On Kummer's memoir of 1857 (*Proceedings of the national Academy of science Washington*, vol. VI, 1920).

A property of cyclotomic integers and its relation with Fermat's last theorem (*Annals of Mathematics*, vol. XXI, p. 73, 1920).

Même titre (second mémoire) (*Annals of Mathematics*, vol. XXVI, p. 217, 1925).

A new type of criteria for the first case of the last Fermat's theorem (*Annals of Mathematics*, vol. XXVI, p. 88, 1925).

Transformation of the Kummer's criteria (*Annals of Mathematics*, vol. XXVII, p. 171, 1926 ; vol. XXVIII, p. 151, 1927).

Note on trinomial congruences and the first case of the

Fermat's last theorem (*Annals of Mathematics*, vol. XXVII, p. 54, 1926).

An algorithm for transforming Kummer criteria in connection with Fermat's last theorem (*Annals of Mathematics*, vol. XXX, 1929).

§ VII. — Sur le dernier théorème de Fermat,

par L.-J. Mordell, 1929.

L'auteur démontre que les nombres $a+bi$ ne peuvent être décomposés en facteurs premiers, tels qu'il les a définis, que d'une seule manière.

Il résout ainsi l'équation $x^2+y^2=z^n$: on a

$$(x+yi)(x-yi)=z^n,$$

d'où $x+yi=i^r(a+bi)^n, \qquad x-yi=i^{-r}(a-bi)^n,$

$$z=a^2+b^2,$$

a, b entiers, r entier quelconque (1).

Viennent ensuite des entiers algébriques d'un type plus général, pour lesquels une nouvelle définition des nombres premiers est nécessaire et auxquels le théorème sur la décomposition unique est inapplicable.

De ces entiers algébriques, il passe à l'équation

$$(x+y)(x+\alpha y)(x+\alpha^2 y)\ldots(x+\alpha^{p-1}y)=z^p,$$

α, racine p^{ieme} de l'unité. « On ne peut pas affirmer que $x+\alpha y$, par exemple, est la $p^{i\grave{e}me}$ puissance d'un nombre complexe de forme $a+b\alpha+\cdots+h\alpha^{p-1}$; de là, l'introduc-

---

(1) Comme x, y peuvent être pris l'un pour l'autre et que leurs signes n'importent pas, on peut réduire les deux formules à une seule

$$x+yi=(a+bi)^n.$$

Les modules des deux membres étant égaux, on aura

$$x^2+y^2=(a^2+b^2)^n.$$

Quant aux valeurs de x, y, z, ce sont

$$x=a^n-C_n^2a^{n-2}b^2+\cdots, \qquad y=C_n^1a^{n-1}b-\cdots, \qquad z=a^2+b^2.$$

tion des nombres idéaux, et l'établissement des relations $x + xy = \xi_1 \tau_1^2$, $x + x^2 y = \xi_2 \tau_2^2$, ... où τ_1, τ_2 ... sont des nombres idéaux et ξ_1, ξ_2 ... des unités complexes. C'est à l'aide de ces relations qu'on parvient au résultat de Kummer. »

« Pendant les cinquante années qui suivirent les travaux de Kummer, on fit très peu de chose pour étendre ou développer leurs conséquences. Ils furent repris après 1900, et en particulier celui-ci : si $x^p + y^p = z^p$ a des solutions premières à p,

$$B_n \frac{d^{p-2n}}{dv^{p-2n}} \left[L(x + e^v y)\right]_{v=0} \equiv 0 \quad (\text{mod. } p),$$

pour $n = 1, 2, 3, \cdots \frac{1}{2}(p-3)$, ou, sous une autre forme, pour $i = 3, 5 \ldots p-4, p-2$,

$$B_{\frac{1}{2}(p-i)} \frac{d^i}{dv^i} \left[L(x + e^v y)\right]_{v=0} \equiv 0 \quad (\text{mod. } p).$$

« Pour $i = 3$, cette congruence se réduit à

$$B_{\frac{1}{2}(p-3)} xy(x-y) \equiv 0 \quad (\text{mod. } p),$$

et, si $B_{\frac{1}{2}(p-3)}$ n'est pas divisible par p, à

$$xy(x-y) \equiv 0 \quad (\text{mod. } p),$$

et celle-ci, à $\quad x - y \equiv 0 \quad (\text{mod. } p)$.

« De même, $x \equiv z$ (mod. p) ; on en déduit $3x^p \equiv 0$ (mod. p), ce qui est impossible à moins que $p = 3$.

« Donc, l'équation n'est pas soluble en valeurs, premières à p, à moins que $B_{\frac{1}{2}(p-3)}$ ne soit divisible par p.

« De même, en prenant $i = 5, 7, 9$, on trouve que $B_{\frac{1}{2}(p-5)}$, $B_{\frac{1}{2}(p-7)}$, $B_{\frac{1}{2}(p-9)}$ sont divisibles par p. Ceci fut démontré en 1905 par Mirimanoff pour les deux derniers nombres de Bernoulli, par Kummer pour les deux premiers ; la divisibilité de $B_{\frac{1}{2}(p-3)}$ avait été annoncée antérieurement par Cauchy, mais sans démonstration. »

Au sujet du théorème de Sophie Germain, l'auteur s'exprime ainsi : « Supposons qu'on puisse trouver un nombre premier impair q satisfaisant aux deux conditions suivantes :

1° que la congruence $x^p + y^p + z^p \equiv 0 \pmod{q}$ demande que l'une des inconnues soit divisible par q ;

2° qu'aucun entier k ne puisse être trouvé vérifiant la relation $k^p - p \equiv 0 \pmod{q}$.

« Alors, $x^p + y^p + z^p = 0$ ne peut être satisfaite par des entiers premiers à p. »

L'auteur le prouve. Avec $p = 7$, il trouve $q = 29$.

« Le théorème général ci-dessus est dû à Sophie Germain, qui donna le nombre premier q correspondant à tous les nombres premiers p inférieurs à 100. »

Ce travail de M. Mordell avait déjà paru sous le titre *Three lectures on Fermat's last theorem* (*Cambridge University Press*, 1921).

Il fut analysé par M. Eugène Cahen (*Bulletin des Sciences mathématiques*, t. XLV, p. 284, 1921).

Voici une partie de cette analyse.

Marche suivie par Kummer. L'équation $x^p + y^p = z^p$, p premier impair, peut s'écrire

$$(y + x)(y + x\zeta)(y + x\zeta^2) \ldots (y + x\zeta^{p-1}) = z^p,$$

où ζ est une racine $p^{\text{ième}}$ imaginaire de l'unité.

Chacun des facteurs du premier membre est de la forme $x_0 + x_1\zeta + x_2\zeta^2 + \cdots + x_{p-2}\zeta^{p-2}$, x_0, x_1 ... entiers ordinaires. Si l'on pouvait appliquer à ces expressions les règles de la divisibilité des entiers ordinaires et, en particulier, celles de la décomposition en facteurs premiers, on aurait une voie pour aborder le problème. On écrirait que les facteurs du premier membre, s'ils sont premiers deux à deux, sont, chacun, une puissance $p^{\text{ième}}$ parfaite. Mais cela n'est pas vrai en général. Cependant c'est vrai pour tous les $p < 23$. Ce fait explique pourquoi Lamé, Cauchy, et Kummer lui-même au début de ses recherches, avaient l'impression que cela était vrai en général. Kummer avait même donné une

démonstration du théorème de Fermat s'appuyant sur cette supposition erronée. C'est Lejeune-Dirichlet qui l'avertit :

1° que cette supposition avait, en tout cas, besoin d'une démonstration ;

2° qu'à son avis elle était fausse.

Kummer a levé la difficulté par la considération des nombres *idéaux*.

Les nombres idéaux peuvent se définir de bien des manières. M. Mordell a choisi la définition la plus immédiatement accessible. Par contre, cette définition serait peu commode. Kummer a bien remarqué la possibilité d'une définition de cette sorte ; mais ce n'est pas celle qu'il a donnée. La façon dont il procède est bien plus ingénieuse et hardie. Elle consiste à dire qu'un nombre premier ordinaire, non réellement décomposable dans le domaine des entiers du corps $C(\zeta)$, l'est cependant en autant de facteurs idéaux qu'une certaine congruence a de racines. Chaque facteur idéal correspond à une solution de la congruence. On dit qu'un entier du corps est divisible par cet idéal lorsque certaines congruences sont satisfaites.

De la décomposition des nombres premiers ordinaires résulte celle de tous les entiers du corps.

Kummer nous dit que cette conception lui fut suggérée par celle du radical hypothétique ammonium, imaginé en chimie pour expliquer les propriétés basiques de l'ammoniaque.

D'ailleurs, la méthode de Kummer n'est pas absolument rigoureuse ; mais on peut la rendre telle en s'appuyant, par exemple, sur la théorie des congruences à double module de Kronecker.

Les procédés actuels de la Théorie des Nombres donnent des voies plus rapides, peut-être moins claires, pour arriver aux mêmes résultats.

Les idéaux sont (avec Mordell) des expressions de la forme $\sqrt[r]{x_0 + x_1\zeta + \cdots + x_{p-2}\zeta^{p-2}}$, les entiers x étant assujettis à certaines conditions, r étant un entier, *le nombre des classes,* dont la valeur dépend de p. En adjoignant ces nombres

idéaux aux nombres entiers du corps $C(\zeta)$, les lois de la divisibilité ordinaire se trouvent rétablies.

Cela fait, il est relativement simple d'appliquer à $x^p + y^p = z^p$ le procédé employé pour $x^2 + y^2 = z^2$

$$\left| x^2 = (z+y)(z-y), \qquad z+y = m^2, \qquad z-y = n^2, \right.$$

si $$\left. D(z+y,\ z-y) = 1 \right|,$$

si le nombre des classes n'est pas divisible par p.

Pour les valeurs de p satisfaisant à cette condition, Kummer a ainsi démontré l'impossibilité de l'équation non seulement en entiers ordinaires, mais même en entiers du corps $C(\zeta)$, c'est-à-dire qu'il a démontré un théorème plus général que celui de Fermat.

La condition que r n'est pas divisible par p peut se remplacer par une autre.

Posons $$\frac{x}{e^x - 1} = 1 - \frac{x}{2} + \sum_{n=1}^{\infty} (-1)^{n-1} \frac{B_n x^{2n}}{(2n)!},$$

les B_n, nombres de Bernoulli.

Alors la condition peut s'énoncer que : *aucun des* $\frac{p-3}{2}$ *premiers nombres de Bernoulli n'ait son numérateur divisible par p.*

Cette condition est vérifiée pour tous les $p < 100$, sauf pour 37, 59, 67.

Kummer chercha à combler cette lacune. En 1857, il donna une méthode s'appliquant aux nombres premiers satisfaisant à certaines conditions autres que les précédentes, lesquelles conditions s'appliquent justement à 37, 59, 67. Mais il résulte des recherches de M. Vandiver que les démonstrations de Kummer ne sont pas à l'abri de toute critique. Pour $p = 37$, une démonstration rigoureuse a été donnée par M. Mirimanoff.

Kummer a aussi démontré que *l'équation* $x^p + y^p = z^p$ *ne peut avoir de solutions en entiers ordinaires dont aucun ne soit divisible par p, que si les numérateurs de* $B_{\frac{p-3}{2}}$ *et* $B_{\frac{p-5}{2}}$ *sont divisibles par p.*

M. Mirimanoff a étendu ces résultats à $B_{\frac{p-7}{2}}$ et $B_{\frac{p-9}{2}}$, et démontré d'autres résultats du même genre.

Les congruences $a^{p-1} \equiv 1$ (mod. p^2). — Voici des conditions d'un autre genre : il n'existe pas de solutions dont aucune ne soit divisible par p, lorsqu'on n'a pas $a^{p-1} \equiv 1$ (mod. p^2), où $a = 2$, Wieferich ; $a = 3$, Mirimanoff ; $a = 5$, Vandiver ; $a = 2$, 11, 17, Frobenius ; $a = 7$, 13, 19, si $p \equiv -1$ (mod. 6), Frobenius.

Conditions d'un autre genre encore. — Si l'on pouvait trouver une infinité de nombres premiers q tels que $x^p + y^p = z^p$ entraînât que l'un des entiers x, y, z dût être divisible par q, cela démontrerait l'impossibilité de l'équation.

Or, Libri, en 1832, énonça qu'*il n'y a pas une infinité* de tels nombres premiers. Ceci fut prouvé en 1886 par Pellet, et en 1909, indépendamment, par Dickson et par Hurwitz.

Le problème de Fermat a, en somme, été résolu pour *certaines* valeurs de n, satisfaisant à *certaines* conditions. Ces conditions sont que certaines coïncidences numériques compliquées n'aient pas lieu. On conçoit que cela puisse arriver très souvent sans qu'on en puisse inférer que cela arrive toujours. D'ailleurs, ces conditions sont *suffisantes* pour que le théorème de Fermat soit vrai, mais non nécessaires ; de sorte que, lorsqu'elles ne sont pas remplies, on ne sait rien.

Il paraît aussi bien difficile de trouver par tâtonnements des valeurs satisfaisant à l'équation de Fermat et de démontrer ainsi, par le fait, la possibilité de sa résolution. Il résulte, en effet, de théorèmes dont M. Mordell ne parle pas, que les valeurs de x, y, z qui pourraient satisfaire à $x^n + y^n = z^n$ sont limitées inférieurement. Le plus simple est celui de Grünert : *les valeurs positives de x, y, z satisfaisant à $x^n + y^n = z^n$ sont toutes plus grandes que n.*

Pour $n = 59$, le plus petit nombre à essayer serait 60. Or $(60)^{59}$ a 105 chiffres.

Démonstration. Posons $z = x + u$ $(u > 0)$, d'où, après

réductions, $y^n > nx^{n-1}u + \cdots$, et, par suite, $y^n > nx^{n-1}$; de même, $x^n > ny^{n-1}$. Élevons la première inégalité à la puissance n, remplaçons x^n par ny^{n-1} ; on trouve facilement $y > n$. De même $x > n$.

Voici comment M. Cahen termine son intéressante analyse, au sujet de l'intérêt pratique de tous ces problèmes :

« Lorsque, en 1881, l'Académie des sciences de Paris mettait au concours le problème de la décomposition des nombres entiers en une somme de cinq carrés, elle fournissait à Minkowski, qui obtint le prix, l'occasion de commencer ses recherches sur les formes quadratiques et sur leurs substitutions automorphes. Par là, elle contribuait peut-être indirectement aux progrès de l'Électricité, de l'Optique et de toute la Mécanique, puisque le même Minkowski a découvert, depuis, le rapport intime qu'il y a entre cette théorie des substitutions automorphes et celle de la relativité de Lorenz-Einstein. »

§ VIII. — Sur le théorème de Fermat,

par L. Massoutié (5 octobre 1931).

« On peut démontrer que, si p, premier, a la forme $6n - 1$, l'une des indéterminées de l'équation $x^p + y^p + z^p = 0$ est nécessairement divisible par 3.

« On s'appuie sur ce lemme : si n est premier avec 3, on a la congruence $a^{6n-1} \equiv a$ (mod. 3).

« Supposons maintenant que $x^p + y^p + z^p = 0$ admette une solution entière $x = a$, $y = b$, $z = c$, premiers entre eux. Nous aurons donc $a^p + b^p + c^p = 0$, et, par application du lemme, $a + b + c \equiv 0$ (mod. 3).

« Supposons qu'aucun des nombres a, b, c ne soit multiple de 3. A cause de la congruence précédente, a, b, c seront tous les trois, en même temps, de la même forme $3h + 1$ ou $3h - 1$.

« Soit maintenant l'équation $X^3 + PX + Q = 0$ admettant pour racines a^p, b^p, c^p.

« On a $(a^p - b^p)^2(b^p - c^p)^2(c^p - a^p)^2 = -4P^3 - 27Q^2$.

« Comme $P = a^p b^p + b^p c^p + c^p a^p = a^p b^p - c^{2p}$, on aura

(1) $(a^p - b^p)^2(b^p - c^p)^2(c^p - a^p)^2 + 27a^{2p}b^{2p}c^{2p} = 4(c^{2p} - a^p b^p)^3$.

« Il est donc clair que $c^{2p} - a^p b^p$ est un *simple* multiple de 3. En effet, les binomes tels que $(a^p - b^p)^2$ sont des multiples de 9 et leur produit est un multiple de 9^3. Si donc $c^{2p} - a^p b^p$ était un multiple de 9, son cube serait un multiple de 9^3, et, à cause de 27 qui figure dans le premier membre, il n'y aurait pas congruence (mod. 3) et (1) serait impossible.

« D'autre part, on sait que si l'on a $a^p + b^p + c^p = 0$, un seul des trois termes est pair et qu'un des binomes $a^p + b^p$, $b^p + c^p$, $c^p + a^p$ est nécessairement divisible par $2^{p\lambda}$, λ étant un entier positif. Cela fait que l'un des binomes $a^p - b^p$, $b^p - c^p$, $c^p - a^p$ est simplement pair, les deux autres impairs.

« On pourra donc écrire (1) ainsi :

(2) $$\frac{(a^2 - b^2)^2(b^2 - c^2)^2(c^2 - a^2)^2}{4} + 27\frac{a^{2p}b^{2p}c^{2p}}{4} = (c^{2p} - a^p b^p)^3.$$

Mais on a $c^{2p} - a^p b^p = (c^2)^p - (ab)^p = (c^2 - ab)R$, R étant impair et non divisible par 3 ; $c^2 - ab$ est alors un simple multiple de 3. Posons $c^2 - ab = 3u$, u non divisible par 3. On aura $(c^2 - ab)^3 = 27u^3R^3$.

« Divisant les deux membres de (2) par 27, il reste

$$3 . 9U^2 + V^2 = u^3R^3.$$

Le second membre est impair et le premier est de la forme $3x^2 + y^2$. Donc R doit être, lui aussi, de la forme $3x^2 + y^2$; mais nous allons montrer que cela est impossible.

« En effet, R peut s'écrire

$$R = (c^2)^{p-1} + (c^2)^{p-2}ab + (c^2)^{p-3}(ab)^2 + \cdots + c^2(ab)^{p-2} + (ab)^{p-1}.$$

« Or, chacun des termes de R est, en vertu de ce qui a été établi plus haut de a, b, c, relativement au module 3, de la forme $3h + 1$, et R contient $p = 6n - 1$ termes. Donc R sera de la forme $3k + 6n - 1$ ou $3m - 1$; mais, on a aussi $R = f^2 + 3g^2$. On arrive donc à $3m - 1 = f^2 + 3g^2$, égalité impossible.

« Donc, il faut nécessairement supposer que a, b ou c soit un multiple de 3. »

Pour $n=2$, c'est $2ab$ qui est divisible par 3 si a ou b est divisible par 3; sinon, c'est a^2-b^2, car a^2 et b^2 ont la forme $3m+1$.

§ IX. — Nouvelles remarques,

par Léon Pomey (12 octobre 1931).

« Je me propose d'établir que si n est un nombre premier de la forme $6h-1$, l'équation (1) $x_1^n+x_2^n+x_3^n=0$ ne peut être satisfaite par des entiers positifs ou négatifs que si l'un d'eux est divisible par 3.

« En effet, si l'on suppose x_1, x_2, x_3 premiers avec 3, chacun d'eux a la forme $\varepsilon+3\lambda$, $\varepsilon=\pm 1$. Mais en vertu de l'équation, ε_1, ε_2, ε_3 doivent avoir la même valeur ε. Donc $x_i^2-x_jx_k$ est divisible par 3. Or si P désigne le quotient $\dfrac{x_i^{2n}-x_j^nx_k^n}{x_i^2-x_jx_k}$, on a (J. M., 9e série, t. IV, p. 3, 1925)

$$(2)\qquad P=n(x_i^2x_jx_k)^{\frac{n-1}{2}}+\text{mult.}\,(x_i^2-x_jx_k)^2.$$

« Par suite, il vient

$$(3)\qquad P\equiv n\ (\text{mod. } 3).$$

« Mais, d'autre part, on a

$$4(x_i^{2n}-x_j^nx_k^n)=3(x_j^n+x_k^n)^2+(x_j^n-x_k^n)^2\,;$$

expression de la forme a^2+3b^2. Donc les diviseurs positifs du premier membre (et P, notamment) doivent être de cette forme et P doit être congru (mod. 3) à un carré, donc à 1. Par suite, en vertu de la congruence (3), n doit être aussi congru à 1 (mod. 3), ce qui est contraire à l'hypothèse. »

BIBLIOGRAPHIE

Abh. der Berliner Akademie, 1857.
Abhandlungen zur Geschichte der Mathematik, 1910.
Acta Mathematica (Journal de Mittag-Leffler), Stockholm, 1890, 1901, 1903.
Akademie der Wissenschaften, zu München, 1901, 1907.
L'Arithmétique sur les courbes algébriques. Thèse de M. Weill, Paris, 1928.
Nouvelles Annales de Mathématiques de Terquem, Paris, 1847, 1850, 1903, 1911 et tomes II, III.
Annales de la Société scientifique de Bruxelles, 1893, 1894.
Annali di Math. 1905, 1908.
Annali di Scienze matematiche e fisiche, 1855.
Annals of Mathematics, 1915, 1916, 1920, 1925, 1926, 1927, 1929.
Appréciation nouvelle et singulière du caractère de Fermat. Note d'Aristide Marre, Paris, 1883, offerte en don aux Nuovi Lincei, t. 36, 1882.
Archiv der Mathematik und Physik (Leipzig und Berlin), tomes 13, 14, 15, 16, 17 ; 1894, 1895, 1908, 1910.
Association pour l'Avancement des Sciences, Paris, 1897, 1899, 1905, 1909, 1910.
Atti dell' Accademia Pontificia di Nuovi Lincei, Rome, 1882, 1884, 1892.
Bachmann, Das Fermat Problem (1919). — Niedere Zahlentheorie, vol. II, chap. IX ; vol. V, p. 521.
Bendz, Ofver Diophanteske rationen, Upsal, 1902.
Bernoulli (Nombres de) : Bertrand (Joseph), Calcul différentiel, et Lacroix, Calcul intégral, tome III ; Glaischer, Messenger 1876 ; Haussner, Gött. Nach. 1893, Zeitschrift f. Math. ; Adams, J. de Crelle, tome 83.
Bertrand (Joseph), Préface du Calcul des Probabilités.
Beweis der Fermatschen Satzes : Darmstadt, Schlapp, 1908 ; Hamburg, H. Seippel, 1908 ; Dresden, A. Kohler, 1908.
Brassine, Précis des Œuvres mathématiques de Fermat, Toulouse, 1853.
Bulletin de l'Académie royale des Sciences de Belgique, 1886, 1887.
Bulletin de la Société mathématique de France, 1879, 1880.
Bulletin des Sciences mathématiques, 1921.

Carmichael, Analyse indéterminée et théorie des Nombres. Presses Universitaires de France, Paris.
Collected mathematical Papers, 1894, 1895.
Comptes rendus de l'Académie des Sciences de Paris, 1825, 1839, 1843, 1846, 1847, 1850, 1853, 1854, 1857, 1863, 1874, 1876, 1879, 1880, 1884, 1894, 1895, 1896, 1905, 1913, 1923, 1931.
Comptes rendus du Congrès des Mathématiciens, 1900.
Nouvelle Correspondance mathématique de Bruxelles, 1878, 1879.
Deutsche Math., t. 26, 1908.
Egoroff, Le théorème de Fermat, 18 pages, St-Pétersbourg, 1911.
Encyclopédie des Sciences mathématiques. Edition française. Edition allemande, Leipzig, Teubner.
Enseignement mathématique, Paris, 1908, 1909.
Euler Léonhard, *Commentationes arithmeticæ,* 2 vol. — Eléments d'Algèbre, 1774, 2 vol., traduits par G. Garnier, 1807.
Fermat (Samuel). *Opera varia.* Toulouse, 1679. *Diophanti arithmetici libri,* 1670.
Fermat (Œuvres de), par Libri.
Fermat (Œuvres de), publiées en 1891 par P. Tannery et C. Henry. 4 vol. in-4°.
Formule d'Albert Girard, Archiv. 3 et Enzykl. d. Math. Wiss.
Gauss, *Disquisitiones arithmeticæ,* 1801, traduites par Poullet-Delisle, 1807.
Giornale di Matematiche, 1889.
A. Hess, Dresden. A. Kohler, in-8°, 1908.
Hilbert, Die Theorie der algebraischen Zahlkörper, traduite par MM. Got et Lévy.
Histoire des Mathématiques, par Hoeffer, 1886.
Histoire des Mathématiques, par Rouse-Ball et Récréations et Problèmes des temps anciens et modernes, 1888, traduits par Fraud, 1905, et par Fitz-Patrick, 1907.
History of the theory of numbers, de Dickson.
Intermédiaire des Mathématiciens, Paris, 1894, 1895, 1897, 1900, 1901, 1904, 1905, 1906, 1908.
Journal de Crelle, Berlin, 1828, 1832, 1837, 1839, 1845, 1850, 1857, 1892, 1893, 1897, 1908, 1909, 1914.
Journal de Liouville, Paris, 1840, 1843, 1847, 1851, 1856, 1880, 1901, 1925.
Journal de l'Ecole Polytechnique, Paris, 1843.
Journal für Mathematik, 1908.
Journal des Savants, 9 février 1665, contient l'éloge de Fermat.
Landry, Mélanges mathématiques transcendants. Bachelier, Paris, 1853.
Libri, Monographies diverses, n° 9, 1859.
B. Lindt, Ueber das letzte Fermat'sche Satz (Abhandlungen zur Geschichte der Mathematik, 1910).
Martone, Dimostrazione di teorema del Fermat, Catanzaro, Dastoli, 1887.
Mathematische Annalen, 1908.

Messenger of Mathematics, 1876, 1885, 1886, 1894, 1895, 1908.
Mordell, Le dernier théorème de Fermat, traduit par M. Sallin. Les Presses Universitaires de France, 1929.
R. Niewiadomski, Ingénieur, Varsovie, 1909.
Nogell, Collection-Mémorial des Sciences Mathématiques. Gauthier-Villars, 1887.
Periodico di Matematica per l'ensegnamento secundino, 1901.
Proceedings of the Cambridge Philos., t. XXI, 1922.
Proceedings of the London Mathematical Society, 1918, et vol. XVIII, 1919.
Proceedings of the National Academy of Sciences, Washington, 1920.
Quarterly Journal, 1908, 1909.
Reale Istituto Lombardo di scienze e lettere (Rendiconti), 1887.
Recueil moscovite math., 1905.
R. Rubissow, Kiew, 15 pages in-8°, en russe.
Sageret, 8, rue Lamartine, Paris, Dulac, 1909.
Sitzungsberichte der Berliner mathematischen Gesellschaft, 1909-1910.
Sitzungsberichte der math. physikal. Akad. der Wissenschaften, 1901, 1907, 1910, 1912, 1914.
Sommer, Vorlesungen über Zahlentheorie.
Sphynx-Œdipe, par Gérardin, Nancy, 1908, 1909, 1910.
Théorie des Nombres, de Legendre. Editions 1823 et 1830.
Théorie des Nombres, d'Edouard Lucas, 1891.
Théorie des Nombres, d'Eugène Cahen. 1914, 1924, 3e volume en préparation.
Théorie des Nombres, de P. Bachmann, Leipzig, 1902.
Theory of Numbers, de Peter Barlow, 1881.
Vlaches, Berlin, Gotheiner, 1908.
Weigolin, Stuttgart, Enderlin, 1908.

TABLE DES MATIÈRES

CHARTRES. — IMPRIMERIE DURAND, RUE FULBERT (2-1932).